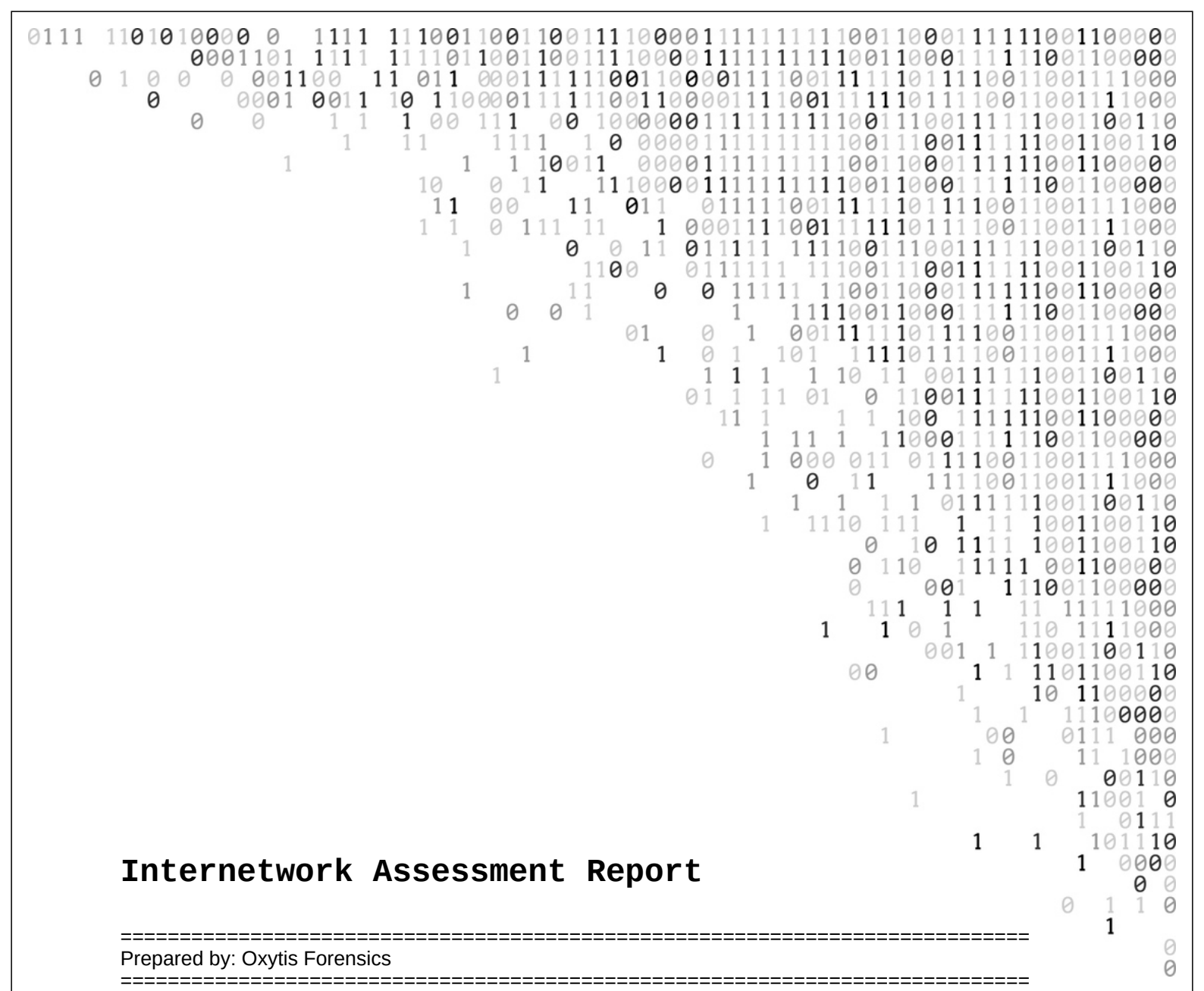


Internetwork Assessment Report

==========
Prepared by: Oxytis Forensics
==========

Example Company

==========
Date: 11 July 2022
==========

Content

1.0 Executive Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Curabitur pretium tincidunt lacus. Nulla gravida orci a odio. Nullam varius, turpis et commodo pharetra, est eros bibendum elit, nec luctus magna felis sollicitudin mauris. Integer in mauris eu nibh euismod gravida. Duis ac tellus et risus vulputate vehicula. Donec lobortis risus a elit. Etiam tempor. Ut ullamcorper, ligula eu tempor congue, eros est euismod turpis, id tincidunt sapien risus a quam. Maecenas fermentum consequat mi. Donec fermentum. Pellentesque malesuada nulla a mi. Duis sapien sem, aliquet nec, commodo eget, consequat quis, neque. Aliquam faucibus, elit ut dictum aliquet, felis nisl adipiscing sapien, sed malesuada diam lacus eget erat. Cras mollis scelerisque nunc. Nullam arcu. Aliquam consequat. Curabitur augue lorem, dapibus quis, laoreet et, pretium ac, nisi. Aenean magna nisl, mollis quis, molestie eu, feugiat in, orci. In hac habitasse platea dictumst.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Curabitur pretium tincidunt lacus. Nulla gravida orci a odio. Nullam varius, turpis et commodo pharetra, est eros bibendum elit, nec luctus magna felis sollicitudin mauris. Integer in mauris eu nibh euismod gravida. Duis ac tellus et risus vulputate vehicula. Donec lobortis risus a elit. Etiam tempor. Ut ullamcorper, ligula eu tempor congue, eros est euismod turpis, id tincidunt sapien risus a quam. Maecenas fermentum consequat mi. Donec fermentum. Pellentesque malesuada nulla a mi. Duis sapien sem, aliquet nec, commodo eget, consequat quis, neque. Aliquam faucibus, elit ut dictum aliquet, felis nisl adipiscing sapien, sed malesuada diam lacus eget erat. Cras mollis scelerisque nunc. Nullam arcu. Aliquam consequat. Curabitur augue lorem, dapibus quis, laoreet et, pretium ac, nisi. Aenean magna nisl, mollis quis, molestie eu, feugiat in, orci. In hac habitasse platea dictumst.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Vulnerability Assessment

- Port scanning to detect potential host vulnerabilities

Penetration and Forensic Network Assessment (IoC)

- Layer 2/3 network inspection
- Passive & active reconnaissance
- OS Fingerprinting
- DNS attacks
- Blacklist & IP reputation discovery
- Credential compromise & Lateral access

OSINT - Open-source intelligence

- Surface web discovery
- Credential harvesting
- Leaked credentials

1.1 Findings

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Curabitur pretium tincidunt lacus. Nulla gravida orci a odio. Nullam varius, turpis et commodo pharetra, est eros bibendum elit, nec luctus magna felis sollicitudin mauris. Integer in mauris eu nibh euismod gravida. Duis ac tellus et risus vulputate vehicula. Donec lobortis risus a elit. Etiam tempor. Ut ullamcorper, ligula eu tempor congue, eros est euismod turpis, id tincidunt sapien risus a quam. Maecenas fermentum consequat mi. Donec fermentum. Pellentesque malesuada nulla a mi. Duis sapien sem, aliquet nec, commodo eget, consequat quis, neque. Aliquam faucibus, elit ut dictum aliquet, felis nisl adipiscing sapien, sed malesuada diam lacus eget erat. Cras mollis scelerisque nunc. Nullam arcu. Aliquam consequat. Curabitur augue lorem, dapibus quis, laoreet et, pretium ac, nisi. Aenean magna nisl, mollis quis, molestie eu, feugiat in, orci. In hac habitasse platea dictumst.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Curabitur pretium tincidunt lacus. Nulla gravida orci a odio. Nullam varius, turpis et commodo pharetra, est eros bibendum elit, nec luctus magna felis sollicitudin mauris. Integer in mauris eu nibh euismod gravida. Duis ac tellus et risus vulputate vehicula. Donec lobortis risus a elit. Etiam tempor. Ut ullamcorper, ligula eu tempor congue, eros est euismod turpis, id tincidunt sapien risus a quam. Maecenas fermentum consequat mi. Donec fermentum. Pellentesque malesuada nulla a mi. Duis sapien sem, aliquet nec, commodo eget, consequat quis, neque. Aliquam faucibus, elit ut dictum aliquet, felis nisl adipiscing sapien, sed malesuada diam lacus eget erat. Cras mollis scelerisque nunc. Nullam arcu. Aliquam consequat. Curabitur augue lorem, dapibus quis, laoreet et, pretium ac, nisi. Aenean magna nisl, mollis quis, molestie eu, feugiat in, orci. In hac habitasse platea dictumst.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Curabitur pretium tincidunt lacus. Nulla gravida orci a odio. Nullam varius, turpis et commodo pharetra, est eros bibendum elit, nec luctus magna felis sollicitudin mauris. Integer in mauris eu nibh euismod gravida. Duis ac tellus et risus vulputate vehicula. Donec lobortis risus a elit. Etiam tempor. Ut ullamcorper, ligula eu tempor congue, eros est euismod turpis, id tincidunt sapien risus a quam. Maecenas fermentum consequat mi. Donec fermentum. Pellentesque malesuada nulla a mi. Duis sapien sem, aliquet nec, commodo eget, consequat quis, neque. Aliquam faucibus, elit ut dictum aliquet, felis nisl adipiscing sapien, sed malesuada diam lacus eget erat. Cras mollis scelerisque nunc. Nullam arcu. Aliquam consequat. Curabitur augue lorem, dapibus quis, laoreet et, pretium ac, nisi. Aenean magna nisl, mollis quis, molestie eu, feugiat in, orci. In hac habitasse platea dictumst.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Curabitur pretium tincidunt lacus. Nulla gravida orci a odio. Nullam varius, turpis et commodo pharetra, est eros bibendum elit, nec luctus magna felis sollicitudin mauris. Integer in mauris eu nibh euismod gravida. Duis ac tellus et risus vulputate vehicula. Donec lobortis risus a elit. Etiam tempor. Ut ullamcorper, ligula eu tempor congue, eros est euismod turpis, id tincidunt sapien risus a quam. Maecenas fermentum consequat mi. Donec fermentum. Pellentesque malesuada nulla a mi. Duis sapien sem, aliquet nec, commodo eget, consequat quis, neque. Aliquam faucibus, elit ut dictum aliquet, felis nisl adipiscing sapien, sed malesuada diam lacus eget erat. Cras mollis scelerisque nunc. Nullam arcu. Aliquam consequat. Curabitur augue lorem, dapibus quis, laoreet et, pretium ac, nisi. Aenean magna nisl, mollis quis, molestie eu, feugiat in, orci. In hac habitasse platea dictumst.

1.2 Recommendations

* Lorem ipsum dolor sit amet, consectetur adipiscing elit
* Curabitur pretium tincidunt lacus
* Aenean magna nisl, mollis quis, molestie eu
* Lorem ipsum dolor sit amet, consectetur adipiscing elit

2.0 Penetration Testing

Oxytis Forensics lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Curabitur pretium tincidunt lacus. Nulla gravida orci a odio. Nullam varius, turpis et commodo pharetra, est eros bibendum elit, nec luctus magna felis sollicitudin mauris. Integer in mauris eu nibh euismod gravida. Duis ac tellus et risus vulputate vehicula. Donec lobortis risus a elit. Etiam tempor. Ut ullamcorper, ligula eu tempor congue, eros est euismod turpis, id tincidunt sapien risus a quam. Maecenas fermentum consequat mi. Donec fermentum. Pellentesque malesuada nulla a mi. Duis sapien sem, aliquet nec, commodo eget, consequat quis, neque. Aliquam faucibus, elit ut dictum aliquet, felis nisl adipiscing sapien, sed malesuada diam lacus eget erat. Cras mollis scelerisque nunc. Nullam arcu. Aliquam consequat. Curabitur augue lorem, dapibus quis, laoreet et, pretium ac, nisi. Aenean magna nisl, mollis quis, molestie eu, feugiat in, orci. In hac habitasse platea dictumst.

2.1 Compromise Analysis

In hac habitasse platea dictumst:

Linux 2.6.x
Windows 7 or 8
Windows NT kernel
Windows NT kernel 5.x

In hac habitasse platea dictumst:

In hac habitasse platea dictumst:

In hac habitasse platea dictumst:

192.168.1.1

In hac habitasse platea dictumst:

In hac habitasse platea dictumst:

In hac habitasse platea dictumst:

In hac habitasse platea dictumst:

In hac habitasse platea dictumst:

In hac habitasse platea dictumst:

1 France
1 Ireland
3 Italy
1 Japan
15 Netherlands
1 United Kingdom
148 United States

In hac habitasse platea dictumst:

7 Akamai Technologies, Inc.
13 Amazon.com, Inc.
63 Amazon Technologies Inc.
7 Facebook, Inc.

2 Google LLC
1 Level 3 Parent, LLC
3 Microsoft Corporation
3 Red Hat, Inc.
1 StackPath, LLC.
1 Sucuri

Credentials Harvested:

192.168.1.50 TCP 80 USER: acme_user PASS: acme_password

3.0 External Discovery

Oxytis Forensics OSINT methods attempt to discover leaked credentials and other incidental data. During OSINT we search for use of credentials in other third party services that could have minimal security protection and consequently offer an opportunity for attackers. We also look for indication of phishing services that are set up to appear to belong to Example. Oxytis Forensics attempts to find incidental or leaked documents that reside in places like pastebin, forums, search engines, and various social media sites. For example, monitoring Internet sites known to traffic information about organizational data on the dark web and open Internet could reveal active campaigns in progress.

Subdomains Registered: 4100

34-ws-feed.sandbox.exchange
qa5.developer.sandbox.exchange
a68.ws-feed.sandbox.exchange
distilleryvesper8.sandbox.exchange
public-index.sandbox.exchange
meechumlocalproxy.sandbox.exchange
ccm
jean.public.sandbox.exchange
02api.sandbox.exchange
api.learned.sandbox.exchange
pcbang.sandbox.exchange
fpdbs.sandbox.exchange
ws-feedbeastmode.sandbox.exchange
a30.sandbox.exchange
505189097486comet.papi-content-photos7.sandbox.exchange
zcash-indexer
publica74.sandbox.exchange
api-public13.sandbox.exchange
public.it.sandbox.exchange
ws-feed.obs.sandbox.exchange
pl-api.sandbox.exchange
public.de.sandbox.exchange
trial-public.sandbox.exchange
publicclient20.sandbox.exchange
avpxy01api.sandbox.exchange
...

Domains (Typosquatting): 607

Typosquatting attacks start with cybercriminals buying and registering a domain name that is either a misspelling, alternative spelling, hyphenated, or wrong domain ending .

['coinbase.sale', 'coinbase.studio', 'xn--coinba-14a98c.com', 'xn--cobase-xt7bx7b.com', 'xn--coinbse-30c.gq', 'coinbase.one', 'xn--onbase-vua3c.com', 'coinbase.works', 'coinbase.engineering', 'coinbase.com.au', 'xn--cinbase-92c.com', 'coinbase.to', 'xn--cinbase-q1a.com', 'xn--coibase-fjd.com', 'xn--coinbas-bu4c.com', 'coinbase.cyou', 'xn--coinbas-z8a.com', 'xn--conbase-veb.com', 'xn--cinbas-gva2h.com', 'xn--coinbse-9wa.com', 'xn--conbase-sfb.com', 'coinbase.io', 'coinbase.beer', 'coinbase.trading', 'coinbase.ir', 'xn--coinbas-xs4c.name', 'coinbase.net.in', 'xn--cnbase-3va9c.com', 'xn--conbase-0ya.com', 'coinbase.re', 'xn--cinbase-d5b.com', 'coinbase.exposed', 'coinbase.ch', 'coinbase.cf', 'coinbase.xn--kprw13d', 'coinbase.support', 'coinbase.om', 'coinbase.care', 'coinbase.gdn', 'coinbase.community', 'xn--coinbas-ov4c.com', 'xn--coinbas-9r7e.com', 'xn--conbase-pza.name', 'xn--coibase-5jb.com', 'xn--coinase-5m3c.com', 'xn--coinbas-pya.com', 'xn--coibase-2kb.com', 'xn--oinbase-15a.cc', 'xn--cinbase-khc.com', 'coinbase.today', 'coinbase.fit', 'coinbase.monster', 'xn--conbse-4va8491d.com', 'coinbase.international', 'coinbase.ag', 'coinbase.software', 'xn--cnbs-ssa3i5gvk.com', 'xn--cnbse-hwa50akj.com', 'xn--cinbase-5lb.com', 'xn--coinbse-lq4c.com', 'coinbase.limited', 'coinbase.land', 'coinbase.nz', 'xn--cinbas-gva8i.com', 'coinbase.game', 'xn--cinbase-223c.com', 'xn--coibase-o23c.com', 'xn--coinbse-ru2c.com', 'coinbase.gy', 'coinbase.vg', 'coinbase.sg', 'coinbase.fish', 'xn--coinbae-nt2c.com', 'xn--coinase-lyb.com', 'coinbase.mobi', 'xn--coinbas-ut4c.com', 'coinbase.business', 'coinbase.dev', 'xn--conbse-x1c6198c.com', 'coinbase.es', 'xn--cinbase-d5b.net', 'xn--conbase-ww4c.net', 'coinbase.ie', 'coinbase.email', 'xn--coinbas-27a.com', 'coinbase.exchange', 'xn--conbase-vgd.net', 'xn--conbase-sfb.net', 'coinbase.icu', 'coinbase.reviews', 'coinbase.properties', 'coinbase.pm', 'xn--coinbse-ir4c.com', 'coinbase.in', 'xn--2fghl0e9ewfucwh.com', 'coinbase.sc', 'coinbase.tk', 'xn--conbase-hza.com', 'xn--oinbase-in3c.com', 'xn--coinbae-ypb.com', 'xn--coinbae-873c.com', 'xn--coinbse-twa.com', 'xn--cobase-cwa8121d.com', 'coinbase.com.tw', 'coinbase.cn', 'xn--cinbase-mz4c.com', 'xn--coibase-q4b.com', 'xn--cinbase-g43c.com', 'xn--coinbas-ru4c.com', 'xn--conbase-5tc.com', 'coinbase.cool', 'xn--coinbse-tl3c.com', 'coinbase.property', 'coinbase.management', 'coinbase.live', 'coinbase.st', 'coinbase.lol', 'xn--oinbase-15a.cf', 'coinbase.sx', 'coinbase.de', 'coinbase.party', 'xn--coinbse-30c.ml', 'xn--conbas-gva1a.com', 'xn--coinbas-z8a.xyz', 'coinbase.guide', 'coinbase.wiki', 'coinbase.tax', 'xn--coinase-4bd.net', 'xn--coinbas-j8a.net', 'xn--coinbse-t4a.com', 'xn--conbas-uva1a.com', 'coinbase.bz', 'coinbase.farm', 'xn--coinbas-z8a.info', 'coinbase.vn', 'coinbase.tc', 'coinbase.auction', 'coinbase.horse', 'coinbase.wf', 'coinbase.rocks', 'coinbase.website',

'xn--coinbas-tr3c.name', 'xn--coinase-4bd.com', 'xn--coinbae-vqb.com', 'xn--coinbse-ixa.com', 'xn--coinbas-xs4c.com', 'xn--oinbase-15a.com', 'coinbase.je', 'xn--coinbas-hya.app', 'xn--cnbase-i8a5y.com', 'xn--coinbas-w9a.com', 'coinbase.inc', 'coinbase.gifts', 'coinbase.pizza', 'coinbase.ga', 'coinbase.asia', 'xn--coinbse-30c.ga', 'xn--cinbse-zc8bxn.com', 'xn--cinbs-iwa1kvt.com', 'xn--oinbase-i6a.com', 'xn--coinbas-m1c.com', 'coinbase.li', 'coinbase.mn', 'coinbase.com.cn', 'coinbase.cat', 'xn--coibase-mn2c.com', 'xn--conbase-8ya.net', 'xn--conbase-sv3c.com', 'coinbase.tn', 'coinbase.moe', 'coinbase.pe', 'xn--cibase-3wb7879c.com', 'xn--cinbase-sx4c.com', 'xn--conbase-ww4c.com', 'xn--conbase-feb.com', 'xn--coinbse-rgc.com', 'coinbase.fr', 'xn--conbase-0ya.link', 'coinbase.cash', 'xn--cinbse-sta4l.com', 'xn--cinbase-2mb.com', 'xn--conbase-cfb.net', 'xn--coibase-jqc.com', 'xn--oinbase-l5a.com', 'coinbase.info', 'coinbase.tattoo', 'coinbase.ink', 'coinbase.institute', 'coinbase.social', 'coinbase.ec', 'coinbase.bot', 'coinbase.co.ke', 'coinbase.insure', 'coinbase.name', 'coinbase.frl', 'coinbase.yoga', 'coinbase.biz', 'xn--cinbase-l0a.com', 'xn--coinbas-j8a.com', 'coinbase.compare', 'xn--coinbae-m6c.com', 'coinbase.com.pe', 'xn--cinbase-1uc.com', 'xn--cinbase-mmb.com', 'xn--coinbas-wq3c.com', 'xn--cinbase-tjd.com', 'coinbase.tube', 'coinbase.co', 'coinbase.bond', 'coinbase.loan', 'coinbase.black', 'coinbase.nu', 'coinbase.site', 'xn--conbase-8ya.online', 'xn--coinbas-hya.co', 'xn--coinbse-7o4c.com', 'xn--coinbse-4p4c.com', 'xn--coinbas-utc.com', 'coinbase.feedback', 'coinbase.com.hk', 'xn--onbase-vua5b.com', 'coinbase.chat', 'coinbase.tokyo', 'coinbase.coupons', 'xn--coibas-yt7b11b.com', 'coinbase.gratis', 'coinbase.news', 'coinbase.cafe', 'xn--cinbase-py4c.com', 'xn--cinbase-ks7e.com', 'xn--coinase-qm2c.com', 'coinbase.net.nz', 'coinbase.ovh', 'coinbase.red', 'xn--cinbse-eua4l.com', 'xn--coinbse-lwa.com', 'xn--coinbae-s73c.com', 'coinbase.fi', 'coinbase.ceo', 'coinbase.video', 'coinbase.app', 'coinbase.com.ua', 'coinbase.games', 'xn--onbase-21a3402d.com', 'coinbase.media', 'coinbase.pet', 'xn--coinase-pm3c.com', 'coinbase.ar', 'coinbase.fyi', 'xn--cinbase-g14c.com', 'xn--coinbas-etc.com', 'coinbase.store', 'coinbase.gd', 'coinbase.global', 'coinbase.finance', 'coinbase.tech', 'coinbase.se', 'coinbase.host', 'coinbase.com', 'coinbase.love', 'coinbase.services', 'xn--coibase-83c.com', 'coinbase.com.ht', 'coinbase.com.sg', 'coinbase.how', 'xn--onbase-vua1d.com', 'xn--cinbase-d0a.com', 'xn--coinbas-9r3c.com', 'coinbase.org', 'coinbase.am', 'coinbase.nom.za', 'xn--coinbse-30c.cf', 'coinbase.tw', 'coinbase.agency', 'coinbase.dog', 'coinbase.au', 'coinbase.xn--fiqs8s', 'xn--coinase-wxb.com', 'xn--conbase-9v2c.com', 'xn--coibase-b13c.com', 'xn--coinbse-op4c.com', 'coinbase.vip', 'coinbase.sk', 'xn--coinbas-xya.net', 'coinbase.id', 'coinbase.pro', 'coinbase.la', 'coinbase.net', 'coinbase.pl', 'coinbase.space', 'coinbase.co.in', 'xn--cinbase-9mc.com', 'coinbase.plus', 'coinbase.kred', 'coinbase.org.ph', 'xn--conbas-q9a8951d.com', 'xn--coinbae-mo2c.com', 'coinbase.money', 'xn--coinbae-p83c.com', 'coinbase.menu', 'xn--coinbae-xmd.com', 'xn--coinbas-xya.com', 'xn--coibase-mkb.com', 'xn--cinbse-lua6k.com', 'xn--cinbase-z04c.com', 'xn--conbase-8v3c.com', 'coinbase.click', 'coinbase.contact', 'coinbase.si', 'coinbase.promo', 'coinbase.careers', 'xn--coinbas-g9a.net', 'xn--coinbas-xs4c.net', 'coinbase.be', 'coinbase.company', 'coinbase.com.im', 'xn--coibase-6za.com', 'coinbase.lu', 'xn--coinbse-9wa.site', 'xn--conbse-6za74a.com', 'coinbase.mu', 'coinbase.com.my', 'coinbase.legal', 'coinbase.rs', 'xn--coinbas-et4c.com', 'xn--cobase-4va6221d.com', 'xn--cinbae-3wa09f.com', 'coinbase.tools', 'xn--conbse-q9a48q.com', 'coinbase.it', 'coinbase.cam', 'coinbase.fans', 'coinbase.kz', 'coinbase.security', 'xn--cinbase-d0a.net', 'coinbase.gold', 'coinbase.ma', 'coinbase.cards', 'coinbase.select', 'coinbase.ru', 'xn--coibase-6id.com', 'xn--coinbae-m93c.com', 'xn--coinbse-vn7e.com', 'coinbase.casa', 'coinbase.net.ph', 'xn--coinbse-1qc.com', 'coinbase.financial', 'coinbase.com.ng', 'coinbase.wtf', 'coinbase.market', 'coinbase.africa', 'coinbase.world', 'xn--conbase-8ya.com', 'xn--coinbas-z8a.tk', 'coinbase.partners', 'coinbase.science', 'coinbase.pr', 'coinbase.by', 'xn--coinbse-un4c.com', 'xn--cinbase-10a.com', 'xn--cinbase-qnc.com', 'xn--coinbas-hya.com', 'coinbase.com.mx', 'coinbase.bg', 'xn--cinbase-d24c.com', 'xn--oinbase-txa.com', 'xn--coinase-8l3c.com', 'coinbase.capital', 'coinbase.mom', 'coinbase.in.th', 'coinbase.com.co', 'xn--conbase-sfb.name', 'coinbase.xin', 'coinbase.fund', 'xn--cnbase-iwa5a.com', 'xn--oinbse-vua8991d.com', 'coinbase.london', 'coinbase.cfd', 'coinbase.onl', 'coinbase.pink', 'xn--coinbse-nkc.com', 'coinbase.org.in', 'coinbase.me.uk', 'coinbase.zone', 'coinbase.shop', 'xn--conbse-6ta3e.com', 'coinbase.mx', 'coinbase.ist', 'coinbase.team', 'xn--coinase-5m3c.net', 'xn--coinase-br2c.com', 'xn--oinbase-r5c.com', 'xn--cinbase-t2c.com', 'xn--coinbas-8xa.com', 'xn--conbase-vgd.com', 'xn--cinbase-90a.com', 'xn--cinbase-cx4c.com', 'coinbase.co.jp', 'coinbase.ind.in', 'coinbase.pk', 'xn--coinbas-z8a.net', 'coinbase.desi', 'coinbase.blog', 'coinbase.best', 'coinbase.miami', 'xn--conase-q9a5510d.com', 'coinbase.uz', 'coinbase.top', 'coinbase.academy', 'coinbase.ee', 'coinbase.build', 'coinbase.digital', 'coinbase.city', 'coinbase.casino', 'coinbase.claims', 'xn--conbse-cwa4o.com', 'coinbase.ke', 'coinbase.ng', 'coinbase.xn--ngbrx', 'coinbase.cl', 'coinbase.club', 'xn--coinbas-8jc.com', 'xn--coinbse-bo4c.com', 'coinbase.bio', 'coinbase.rest', 'xn--coinbas-g9a.com', 'coinbase.wales', 'coinbase.tv', 'xn--cinbase-2z4c.com', 'xn--cinbase-ivc.com', 'xn--coinbse-ro4c.com', 'xn--oinbase-hcd.com', 'xn--coinbas-iv2c.com', 'coinbase.solutions', 'xn--coinbas-hya.vn', 'xn--cnbase-wva9c.com', 'coinbase.art', 'xn--coibase-713c.com', 'xn--coinbas-7u4c.com', 'coinbase.co.uk', 'coinbase.events', 'coinbase.as', 'coinbase.ai', 'xn--coinbse-w3a.com', 'xn--cinbase-d2c.com', 'coinbase.at', 'coinbase.is', 'coinbase.tips', 'coinbase.link', 'xn--conbas-4va45a.com', 'coinbase.fun', 'xn--conbase-pza.com', 'xn--conbase-gw4c.com', 'coinbase.al', 'xn--coinbs-tta9d.com', 'xn--conbas-4va07a.com', 'coinbase.investments', 'coinbase.llc', 'coinbase.uk', 'xn--conbase-sfb.ws', 'coinbase.net.au', 'coinbase.cc', 'coinbase.page', 'coinbase.nyc', 'coinbase.boston', 'xn--cinbase-urc.com', 'xn--coinbae-xxc.com', 'xn--coinbse-en4c.net', 'xn--coinbas-hya.net', 'xn--cinbase-w14c.com', 'xn--coinbas-z8a.cf', 'xn--coinbas-4v4c.com', 'xn--coinbse-fsc.com', 'xn--coibase-mkb.net', 'coinbase.ltd', 'coinbase.tel', 'coinbase.im', 'xn--conbase-ydb.com', 'coinbase.af', 'coinbase.amsterdam', 'coinbase.cab', 'coinbase.ren', 'coinbase.ventures', 'xn--coibae-yt7b8i.com', 'coinbase.ht', 'xn--coinbse-fs4c.com', 'xn--cinbase-t0a.com', 'xn--coinbas-z8a.gq', 'xn--cnbase-wva1c.com', 'xn--coinbs-mta5f.com', 'xn--cinbas-gva8e.com', 'xn--coinbse-d4a.com', 'coinbase.sh', 'coinbase.center', 'xn--coinbae-583c.com', 'coinbase.com.bd', 'coinbase.online', 'coinbase.systems', 'coinbase.su', 'xn--coinase-pm3c.name', 'coinbase.surf', 'xn--conbase-muc.com', 'xn--coibase-vs2c.com', 'coinbase.cz', 'coinbase.com.pl', 'coinbase.jp', 'xn--cnbas-mza7nvk.com', 'coinbase.wang', 'xn--coinbse-en4c.com', 'coinbase.ca', 'coinbase.com.es', 'coinbase.us', 'coinbase.net.cn', 'xn--coinbse-30c.tk', 'coinbase.cm', 'xn--coinbse-dwa.com', 'coinbase.eu', 'coinbase.ro', 'coinbase.discount', 'coinbase.directory', 'coinbase.krd', 'xn--cinbase-j33c.com', 'xn--coinbse-1q4c.com', 'coinbase.com.bz', 'coinbase.group', 'coinbase.technology', 'coinbase.bet', 'coinbase.study', 'coinbase.kim', 'coinbase.dk', 'xn--oinbase-44a.com', 'xn--coinbse-vsc.com', 'xn--cinbase-w1c.com', 'coinbase.run', 'coinbase.cloud', 'coinbase.luxe', 'coinbase.org.uk', 'coinbase.no', 'coinbase.deals', 'xn--coinbae-fqb.com', 'coinbase.xn--kpry57d', 'coinbase.xyz', 'coinbase.work', 'coinbase.fm', 'coinbase.gift',

'coinbase.life', 'coinbase.hk', 'coinbase.foundation', 'coinbase.cq.cn', 'coinbase.ninja', 'xn--conbas-xva87a.com', 'coinbase.coach', 'coinbase.ge', 'coinbase.guru', 'xn--coinbse-yr4c.com', 'coinbase.report', 'xn--coinbas-dr3c.com', 'xn--coibase-rlb.com', 'coinbase.sucks', 'coinbase.expert', 'xn--coinbse-30c.com', 'xn--coibase-r13c.com', 'xn--coinbse-1wa.com', 'xn--conbase-4gc.com', 'coinbase.rip', 'xn--oinbase-44a.name', 'xn--2fgdr0ezesg4b3j.com', 'xn--coinbs-mua7a.com', 'coinbase.baby', 'xn--cinbase-8x4c.com', 'coinbase.markets', 'coinbase.credit', 'coinbase.coffee', 'coinbase.uno', 'coinbase.network', 'coinbase.loans', 'coinbase.help', 'coinbase.or.kr', 'coinbase.press', 'coinbase.training', 'coinbase.express', 'coinbase.me', 'coinbase.blue', 'coinbase.army', 'coinbase.codes', 'coinbase.gives', 'coinbase.pub', 'xn--cinbase-5y4c.com', 'xn--coinbse-30c.net', 'xn--coibase-b13c.net', 'xn--coinbas-gq3c.com', 'xn--coinbse-3kc.com', 'coinbase.pt', 'xn--cinbase-z33c.com', 'xn--oinbase-mzb.com', 'xn--cnbase-bl8bpa.com', 'coinbase.car', 'coinbase.design', 'xn--coinbas-tr3c.com', 'coinbase.eco', 'xn--cinbase-j04c.com', 'xn--conbase-cfb.com', 'coinbase.cx', 'coinbase.vc', 'coinbase.camp', 'coinbase.buzz', 'coinbase.fail']

Leaked Credentials: 2

A breach in this context is defined as an incident where data has been unintentionally exposed to the public. The Oxytis Forensics dark web monitoring and reputation management services are designed to monitor, detect and potentially suppress or remove unwanted information on the web.

brian@coinbase.com
- Apollo
- db8151dd
- PDL
- ElasticsearchSalesLeads
- Exactis
- Gravatar
- Ledger
- NetProspex
- Playbook
- VerificationsIO
- YouveBeenScraped

amy.yin@coinbase.com
- Adapt
- Apollo
- PDL
- LinkedInScrape

4.0 Vulnerability Assessment Summary

After accounting for denial of service possibilities where systems can be rendered unresponsive, other specialized conditions can make the below services viable to exploit conditions that allow for compromise where either a reverse shell can be returned, a malicious payload injected, or disclosure of information is possible.

This curated list is based in general on malware potential, sensitivity of information exposure, and insecure use of protocols and services that can result in credential exposure or other general compromise.

Finding	Family	Severity
Unix Operating System Unsupported Version Detection	General	4
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Windows	4
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	Windows	3
Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	3
SMB Signing not required	Misc.	2
Unencrypted Telnet Server	Misc.	2

4 = Critical, **3** = High, **2** = Medium, **1** = Low

by Subnet	Hosts with Exploits	Total Vulnerabilities
172.16.11.0/24	7	240

4.1 Issue Identification and Exploitation

Vulnerabilities identified during the reconnaissance, information discovery, and vulnerability assessment phases such as deep web, social media, and overall Internet footprint are exploited to gain a specified level of access to the target.

Vulnerabilities are mapped to known malware and exploit code discovered on the Internet. These are possible attack vectors where Example has a potential vulnerability to known exploits. The following table displays the distribution of the more relevant vulnerabilities that were identified as having malware and/or exploit code associated with them.

Top Exploits	
Title	Hosts
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	1
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	1

Top Malware	
Title	Hosts
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	1
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	1

The above exploit and malware information is useful to discover indicators of potential malware in the environment or active exploitation looking for specific indicators of the variants of malware or activity with those characteristics and various call-home mechanisms each would employ.

Cleartext protocols:

['tcp/445', 'tcp/80', 'tcp/21', 'tcp/23', 'udp/2049', 'udp/161']

Possible trojan/backdoor/pup ports in in use:

['tcp/50000']

Nonstandard protocol detection/pup:

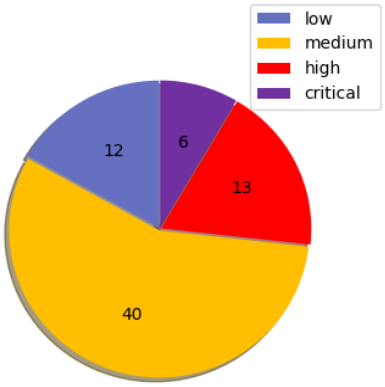
172.16.11.103 --http/5985
172.16.11.109 --http/5985
172.16.11.105 --http/5985
172.16.11.32 --http/10243

172.16.11.55 --http/631
172.16.11.152 --http/5985
172.16.11.2 --http/262
172.16.11.55 --http/280
172.16.11.108 --http/5985
172.16.11.2 --http/260
172.16.11.60 --http/8000
172.16.11.23 --http/5985
172.16.11.32 --http/5357
172.16.11.32 --http/2869
172.16.11.154 --http/5985
172.16.11.24 --http/6002
172.16.11.57 --http/631
172.16.11.153 --http/5985
172.16.11.151 --http/5985

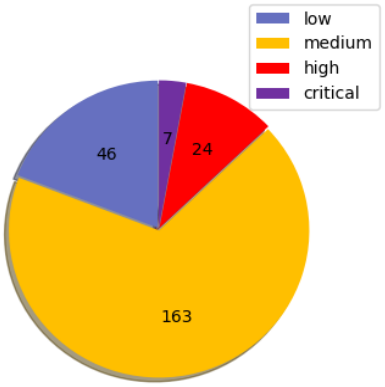
These services should be reviewed by IT staff to ensure the cleartext protocols are necessary for functionality and that the possible backdoor ports are due to implementation of known services.

5.0 Vulnerability Assessment Detail

The 'by Type' chart displays the number of different types of vulnerability grouped by severity level. The 'Totals of each Type' is the aggregate total number of vulnerabilities by severity level. Numerous medium level severity issues could indicate routine maintenance is needed. Typically, these are SSL related issues and often expected in internal environments:

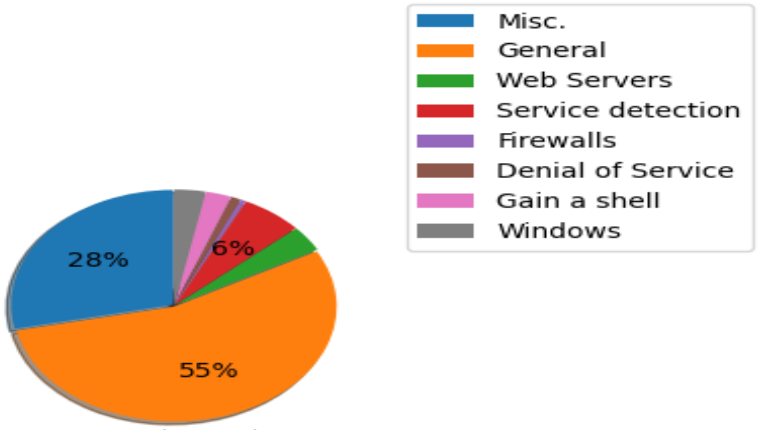


by Type



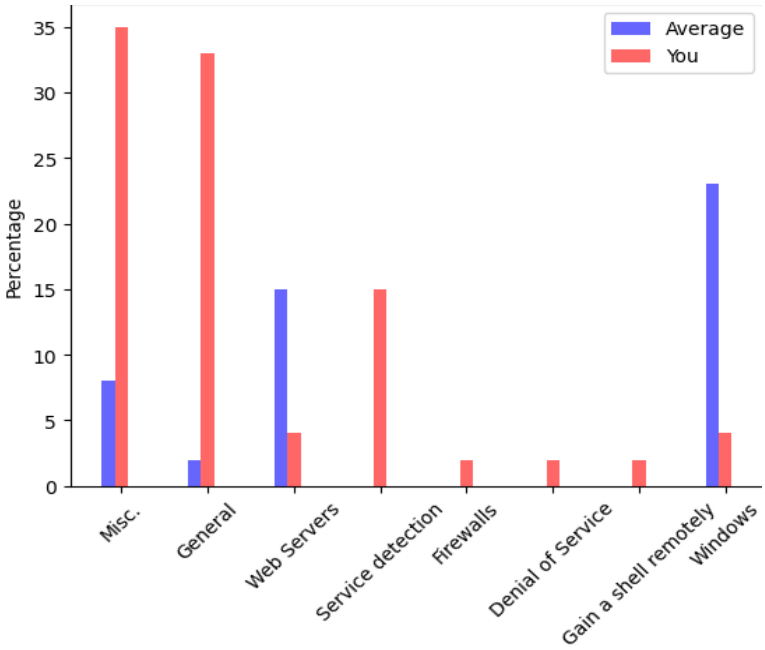
Totals of each Type

The 'by Service' chart displays the distribution of vulnerabilities as a percentage grouped by service type:



by Service

Average comparison of results presented as a percentage of the total of high severity or greater vulnerabilities found, to other organizations of any size that have a similar category of issues:



Critical Findings		
Vulnerability	**Count**	**Severity**
Unix Operating System Unsupported Version Detection	2	4
Description		
According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.		
Output		

`Red Hat Enterprise Linux 4 support ended on 2012-02-29.`
`Upgrade to Red Hat Enterprise Linux 7 / 6.`
 	
`For more information, see : https://access.redhat.com/support/policy/updates/errata/`		

Remediation		
Upgrade to a version of the Unix operating system that is currently supported.		
Affected hosts		
172.16.11.30, 172.16.11.26		
References		

Vulnerability	**Count**	**Severity**
OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation	1	4
Description		
You are running a version of OpenSSH which is older than 3.1. Versions prior than 3.1 are vulnerable to an off by one error that allows local users to gain root access, and it may be possible for remote users to similarly compromise the daemon for remote access. In addition, a vulnerable SSH client may be compromised by connecting to a malicious SSH daemon that exploits this vulnerability in the client code, thus compromising the client system.		
Output		
`No output recorded`		
Remediation		
Upgrade to OpenSSH 3.1 or apply the patch for prior versions. (See: http://www.openssh.org)		
Affected hosts		
172.16.11.2		
References		

Vulnerability	**Count**	**Severity**
OpenSSH < 3.4 Multiple Remote Overflows	1	4
Description		
According to its banner, the remote host appears to be running OpenSSH version 3.4 or older. Such versions are reportedly affected by multiple flaws. An attacker may exploit these vulnerabilities to gain a shell on the remote system. Note that several distributions patched this hole without changing the version number of OpenSSH. Since Oxytis Forensics solely relied on the banner of the remote SSH server to perform this check, this might be a false positive. If you are running a RedHat host, make sure that the command : rpm -q openssh-server Returns : openssh-server-3.1p1-6		
Output		
`No output recorded`		
Remediation		
Upgrade to OpenSSH 3.4 or contact your vendor for a patch.		
Affected hosts		
172.16.11.2		
References		

http://www.openssh.com/txt/preauth.adv

Vulnerability	Count	Severity
OpenSSH < 3.7.1 Multiple Vulnerabilities	1	4

Description

According to its banner, the remote SSH server is running a version of OpenSSH older than 3.7.1. Such versions are vulnerable to a flaw in the buffer management functions that might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Oxytis Forensics solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

rpm -q openssh-server

returns :

openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9)

Output

```
No output recorded
```

Remediation

Upgrade to OpenSSH 3.7.1 or later.

Affected hosts

172.16.11.2

References

https://marc.info/?l=openbsd-misc&m=106375452423794&w=2
https://marc.info/?l=openbsd-misc&m=106375456923804&w=2

Vulnerability	Count	Severity
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	1	4

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Output

```
No output recorded
```

Remediation

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

Affected hosts

172.16.11.24

References

http://www.nessus.org/u?577af692
http://www.nessus.org/u?8e4e0b74

Vulnerability	Count	Severity
VMware ESXi 5.0 < Build 3021432 OpenSLP RCE (VMSA-2015-0007)	1	4

Description

The remote VMware ESXi host is version 5.0 prior to build 3021432. It is, therefore, affected by a remote code execution vulnerability due to a double-free error in the SLPDProcessMessage() function in OpenSLP. An unauthenticated, remote attacker can exploit this, via a crafted package, to execute arbitrary code or cause a denial of service condition.

Output

```
  ESXi version    : ESXi 5.0
  Installed build : 914586
  Fixed build     : 3021432
```

Remediation

Apply patch ESXi500-201510101-SG for ESXi 5.0.

Affected hosts

172.16.11.26

References
https://www.vmware.com/security/advisories/VMSA-2015-0007.html https://www.zerodayinitiative.com/advisories/ZDI-15-455/

High Findings

Vulnerability	Count	Severity
SSH Protocol Version 1 Session Key Retrieval	1	3

Description

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Output

No output recorded

Remediation

Disable compatibility with version 1 of the protocol.

Affected hosts

172.16.11.30

References

Vulnerability	Count	Severity
SSL Version 2 and 3 Protocol Detection	12	3

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Output

- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

```
DES-CBC-MD5              Kx=RSA       Au=RSA     Enc=DES-CBC(56)       Mac=MD5
EXP-RC2-CBC-MD5          Kx=RSA(512)  Au=RSA     Enc=RC2-CBC(40)       Mac=MD5   export
EXP-RC4-MD5              Kx=RSA(512)  Au=RSA     Enc=RC4(40)           Mac=MD5   export
RC4-64-MD5               Kx=RSA       Au=RSA     Enc=RC4(64)           Mac=MD5
```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

```
DES-CBC3-MD5             Kx=RSA       Au=RSA     Enc=3DES-CBC(168)     Mac=MD5
```

High Strength Ciphers (>= 112-bit key)

```
RC2-CBC-MD5              Kx=RSA       Au=RSA     Enc=RC2-CBC(128)      Mac=MD5
RC4-MD5                  Kx=RSA       Au=RSA     Enc=RC4(128)          Mac=MD5
```

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}

Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56) Mac=SHA1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Remediation

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Affected hosts

172.16.11.32, 172.16.11.30, 172.16.11.2, 172.16.11.31, 172.16.11.24, 172.16.11.23, 172.16.11.26

References

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Vulnerability	Count	Severity
OpenSSH < 3.6.1p2 Multiple Vulnerabilities	1	3

Description

According to its banner, the version of OpenSSH running on the remote host is ealier than 3.6.1p2. When compiled for the AIX operating system with a compiler other than that of the native AIX compiler, an error exists that can allow dynamic libraries in the current directory to be loaded before dynamic libraries in the system paths. This behavior can allow local users to escalate privileges by creating, loading and executing their own malicious replacement libraries.

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 3.6.1p2

Remediation

Upgrade to OpenSSH 3.6.1p2 or later.

Affected hosts

172.16.11.2

References

https://www.openssh.com/txt/release-3.6.1p2
https://www.securityfocus.com/archive/1/320038/2003-04-25/2003-05-01/0

Vulnerability	Count	Severity
OpenSSH < 4.5 Multiple Vulnerabilities	1	3

Description

According to its banner, the remote host is running a version of OpenSSH prior to 4.5. Versions before 4.5 are affected by the following vulnerabilities :

- A client-side NULL pointer dereference, caused by a protocol error from a malicious server, which could cause the client to crash. (CVE-2006-4925)

- A privilege separation vulnerability exists, which could allow attackers to bypass authentication. The vulnerability is caused by a design error between privileged processes and their child processes. Note that this particular issue is only exploitable when other vulnerabilities are present. (CVE-2006-5794)

- An attacker that connects to the service before it has finished creating keys could force the keys to be recreated. This could result in a denial of service for any processes that relies on a trust relationship with the server. Note that this particular issue only affects the Apple implementation of OpenSSH on Mac OS X. (CVE-2007-0726)

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 4.5

Remediation

Upgrade to OpenSSH 4.5 or later.
For Mac OS X 10.3, apply Security Update 2007-003.
For Mac OS X 10.4, upgrade to 10.4.9.

Affected hosts

172.16.11.2

References

https://www.openssh.com/txt/release-4.5
https://support.apple.com/kb/TA24626?locale=en_US
https://www.openssh.com/security.html

Vulnerability	Count	Severity
OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities	1	3

Description

According to its banner, the remote host appears to be running OpenSSH version between 2.5.x and 2.9. Such versions reportedly contain multiple vulnerabilities :

- sftp-server does not respect the 'command=' argument of keys in the authorized_keys2 file. (CVE-2001-0816)

- sshd does not properly handle the 'from=' argument of keys in the authorized_keys2 file. If a key of one type (e.g. RSA) is followed by a key of another type (e.g. DSA) then the options for the latter will be applied to the former, including 'from=' restrictions. This problem allows users to circumvent the system policy and login from disallowed source IP addresses. (CVE-2001-1380)

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 2.9.9

Remediation
Upgrade to OpenSSH 2.9.9
Affected hosts
172.16.11.2
References
http://www.openbsd.org/advisories/ssh_option.txt http://www.nessus.org/u?759da6a7 http://www.openssh.com/txt/release-2.9.9

Vulnerability	Count	Severity
OpenSSH < 3.0.2 Multiple Vulnerabilities	1	3

Description

You are running a version of OpenSSH which is older than 3.0.2.
Versions prior than 3.0.2 have the following vulnerabilities :

- When the UseLogin feature is enabled, a local user could export environment variables, resulting in command execution as root. The UseLogin feature is disabled by default. (CVE-2001-0872)

- A local information disclosure vulnerability.
Only FreeBSD hosts are affected by this issue.
(CVE-2001-1029)

Output

No output recorded

Remediation
Upgrade to OpenSSH 3.0.2 or apply the patch for prior versions. (Available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH)
Affected hosts
172.16.11.2
References
https://seclists.org/bugtraq/2001/Sep/208 https://www.freebsd.org/releases/4.4R/errata.html http://www.nessus.org/u?f85ed76c

Vulnerability	Count	Severity
OpenSSH < 3.2.3 YP Netgroups Authentication Bypass	1	3

Description

According to its banner, the version of OpenSSH running on the remote host is older than 3.2.3. It therefore may be affected by an authentication bypass issue. On systems using YP with netgroups, sshd authenticates users via ACL by checking for the requested username and password. Under certain conditions when doing ACL checks, it may instead use the password entry of a different user for authentication. This means unauthorized users could authenticate successfully, and authorized users could be locked out.

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 3.2.3

Remediation
Upgrade to OpenSSH 3.2.3 or later.
Affected hosts
172.16.11.2
References
http://monkey.org/openbsd/archive/bugs/0205/msg00141.html https://www.openssh.com/txt/release-3.2.3 http://www.openbsd.org/errata31.html#sshbsdauth

Vulnerability	Count	Severity
OpenSSH < 3.6.2 Reverse DNS Lookup Bypass	1	3

Description

According to its banner, the remote host appears to be running OpenSSH-portable version 3.6.1 or older.

There is a flaw in such version that could allow an attacker to bypass the access controls set by the administrator of this

server.

OpenSSH features a mechanism that can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups.
If an attacker configures a DNS server to send a numeric IP address when a reverse lookup is performed, this mechanism could be circumvented.

Output

No output recorded

Remediation

Upgrade to OpenSSH 3.6.2 or later.

Affected hosts

172.16.11.2

References

Vulnerability	Count	Severity
OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass	1	3

Description

According to the banner, OpenSSH earlier than 4.7 is running on the remote host. Such versions contain an authentication bypass vulnerability. In the event that OpenSSH cannot create an untrusted cookie for X, for example due to the temporary partition being full, it will use a trusted cookie instead. This allows attackers to violate intended policy and gain privileges by causing their X client to be treated as trusted.

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 4.7

Remediation

Upgrade to OpenSSH 4.7 or later.

Affected hosts

172.16.11.2

References

http://www.openssh.com/txt/release-4.7

Vulnerability	Count	Severity
OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow	1	3

Description

You are running a version of OpenSSH older than OpenSSH 3.2.1.

A buffer overflow exists in the daemon if AFS is enabled on your system, or if the options KerberosTgtPassing or AFSTokenPassing are enabled. Even in this scenario, the vulnerability may be avoided by enabling UsePrivilegeSeparation.

Versions prior to 2.9.9 are vulnerable to a remote root exploit. Versions prior to 3.2.1 are vulnerable to a local root exploit.

Output

No output recorded

Remediation

Upgrade to version 3.2.1 or later.

Affected hosts

172.16.11.2

References

Vulnerability	Count	Severity
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	1	3

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Output

No output recorded

Remediation

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Affected hosts

172.16.11.24

References

http://www.nessus.org/u?68fc8eff
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?065561d0
http://www.nessus.org/u?d9f569cf
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
http://www.nessus.org/u?b9d9ebf9
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Vulnerability	Count	Severity
Microsoft Windows SMBv1 Multiple Vulnerabilities	1	3

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)

- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host

is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.

Output

No output recorded

Remediation

Apply the applicable security update for your Windows version :

- Windows Server 2008 : KB4018466
- Windows 7 : KB4019264
- Windows Server 2008 R2 : KB4019264
- Windows Server 2012 : KB4019216
- Windows 8.1 / RT 8.1. : KB4019215
- Windows Server 2012 R2 : KB4019215
- Windows 10 : KB4019474
- Windows 10 Version 1511 : KB4019473
- Windows 10 Version 1607 : KB4019472
- Windows 10 Version 1703 : KB4016871
- Windows Server 2016 : KB4019472

Affected hosts

172.16.11.24

References

http://www.nessus.org/u?c21268d4
http://www.nessus.org/u?b9253982
http://www.nessus.org/u?23802c83
http://www.nessus.org/u?8313bb60
http://www.nessus.org/u?7677c678
http://www.nessus.org/u?36da236c
http://www.nessus.org/u?0981b934
http://www.nessus.org/u?c88efefa
http://www.nessus.org/u?695bf5cc
http://www.nessus.org/u?459a1e8c
http://www.nessus.org/u?ea45bbc5
http://www.nessus.org/u?4195776a
http://www.nessus.org/u?fbf092cf
http://www.nessus.org/u?8c0cc566

Vulnerability	Count	Severity
ESXi 5.0 < Build 1022489 Multiple Vulnerabilities (remote check)	1	3

Description

The remote VMware ESXi 5.0 host is affected by the following vulnerabilities :

- An off-by-one overflow condition exists in the xmlXPtrEvalXPtrPart() function due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted XML file, to cause a denial of service condition or the execution of arbitrary code. (CVE-2011-3102)

- Multiple integer overflow conditions exist due to improper validation of user-supplied input when handling overly long strings. An unauthenticated, remote attacker can exploit this, via a specially crafted XML file, to cause a denial of service condition or the execution of arbitrary code. (CVE-2012-2807)

- A heap-based underflow condition exists in the bundled libxml2 library due to incorrect parsing of strings not containing an expected space. A remote attacker can exploit this, via a specially crafted XML document, to cause a denial of service condition or the execution of arbitrary code. (CVE-2012-5134)

- A privilege escalation vulnerability exists due to improper handling of control code in the lgtosync.sys driver. A local attacker can exploit this escalate privileges on Windows-based 32-bit guest operating systems. (CVE-2013-3519)

Output

ESXi version : ESXi 5.0
Installed build : 914586
Fixed build : 1022489

Remediation
Apply patch ESXi500-201303101-SG.
Affected hosts
172.16.11.26
References
http://www.nessus.org/u?bac4c6a1 https://www.vmware.com/security/advisories/VMSA-2013-0001.html https://www.vmware.com/security/advisories/VMSA-2013-0004.html https://www.vmware.com/security/advisories/VMSA-2013-0014.html

Medium Findings

Vulnerability	Count	Severity
SMB Signing not required	12	2
Description		
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.		
Output		
No output recorded		
Remediation		
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.		
Affected hosts		
172.16.11.32, 172.16.11.153, 172.16.11.103, 172.16.11.154, 172.16.11.152, 172.16.11.108, 172.16.11.24, 172.16.11.105, 172.16.11.109, 172.16.11.23, 172.16.11.31, 172.16.11.151		
References		
https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea		

Vulnerability	Count	Severity
SSL Certificate Cannot Be Trusted	23	2
Description		
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Oxytis Forensics either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.		
Output		
The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority : |-Subject : CN=CLRK-022.exampleco.net		

|-Issuer : CN=CLRK-022.exampleco.net

Remediation

Purchase or generate a proper certificate for this service.

Affected hosts

172.16.11.32, 172.16.11.30, 172.16.11.2, 172.16.11.153, 172.16.11.103, 172.16.11.154, 172.16.11.31, 172.16.11.152, 172.16.11.108, 172.16.11.24, 172.16.11.105, 172.16.11.109, 172.16.11.23, 172.16.11.26, 172.16.11.151

References

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Vulnerability	Count	Severity
SSL Self-Signed Certificate	19	2

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : CN=CLRK-022.exampleco.net

Remediation

Purchase or generate a proper certificate for this service.

Affected hosts

172.16.11.32, 172.16.11.30, 172.16.11.2, 172.16.11.153, 172.16.11.103, 172.16.11.154, 172.16.11.152, 172.16.11.108, 172.16.11.24, 172.16.11.105, 172.16.11.109, 172.16.11.23, 172.16.11.31, 172.16.11.151

References

Vulnerability	Count	Severity
SSL Medium Strength Cipher Suites Supported (SWEET32)	22	2

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Oxytis Forensics regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Output

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Remediation

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Affected hosts

172.16.11.32, 172.16.11.30, 172.16.11.2, 172.16.11.153, 172.16.11.103, 172.16.11.154, 172.16.11.31, 172.16.11.152,

172.16.11.108, 172.16.11.24, 172.16.11.105, 172.16.11.109, 172.16.11.23, 172.16.11.26, 172.16.11.151

References

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Vulnerability	Count	Severity
Unencrypted Telnet Server	2	2

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Output

Oxytis Forensics collected the following banner from the remote Telnet server :

---------- snip ----------
Red Hat Enterprise Linux ES release 4 (Nahant Update 4)
Kernel 2.6.9-42.0.3.ELsmp on an i686
login:
---------- snip ----------

Remediation

Disable the Telnet service and use SSH instead.

Affected hosts

172.16.11.30, 172.16.11.2

References

Vulnerability	Count	Severity
HTTP TRACE / TRACK Methods Allowed	5	2

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Output

To disable these methods, add the following lines for each virtual
host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Oxytis Forensics sent the following TRACE request :

---------- snip ----------
TRACE /Oxytis Forensics513507486.html HTTP/1.1
Connection: Close
Host: 172.16.11.30
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

---------- snip ----------

and received the following response from the remote server :

---------- snip ----------
HTTP/1.1 200 OK
Date: Fri, 06 Dec 2019 12:01:48 GMT
Server: Apache/2.0.52 (Red Hat)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http

TRACE /Oxytis Forensics513507486.html HTTP/1.1
Connection: Close
Host: 172.16.11.30
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

---------- snip ----------

Remediation

Disable these methods. Refer to the plugin output for more information.

Affected hosts

172.16.11.30, 172.16.11.2

References

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
https://download.oracle.com/sunalerts/1000718.1.html

Vulnerability	Count	Severity
Apache Server ETag Header Information Disclosure	2	2

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

Output

Oxytis Forensics was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source : ETag: "fdcc-f-c1f05a80"
  Inode number : 64972
  File size : 15 bytes

Remediation

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Affected hosts

172.16.11.30

References

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Vulnerability	Count	Severity
SSH Weak Algorithms Supported	3	2

Description

Oxytis Forensics has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Output

The following weak server-to-client encryption algorithms are supported :

  arcfour

The following weak client-to-server encryption algorithms are supported :

arcfour

Remediation

Contact the vendor or consult product documentation to remove the weak ciphers.

Affected hosts

172.16.11.21, 172.16.11.30, 172.16.11.2

References

https://tools.ietf.org/html/rfc4253#section-6.3

Vulnerability	Count	Severity
SSL Certificate Expiry	3	2

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Output

The SSL certificate has already expired :

Subject : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain, emailAddress=root@localhost.localdomain
Issuer : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit, CN=localhost.localdomain, emailAddress=root@localhost.localdomain
Not valid before : Nov 6 19:17:53 2006 GMT
Not valid after : Nov 6 19:17:53 2007 GMT

Remediation

Purchase or generate a new SSL certificate to replace the existing one.

Affected hosts

172.16.11.23, 172.16.11.30

References

Vulnerability	Count	Severity
SSL Certificate Signed Using Weak Hashing Algorithm	11	2

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Oxytis Forensics CA database (known_CA.inc) have been ignored.

Output

The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=localhost.localdomain/E=root@localhost.localdomain
|-Signature Algorithm : MD5 With RSA Encryption
|-Valid From : Nov 06 19:17:53 2006 GMT
|-Valid To : Nov 06 19:17:53 2007 GMT

Remediation

Contact the Certificate Authority to have the certificate reissued.

Affected hosts

172.16.11.32, 172.16.11.30, 172.16.11.2, 172.16.11.31, 172.16.11.24, 172.16.11.23, 172.16.11.26

References
https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba

Vulnerability	Count	Severity
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	12	2

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Output

Oxytis Forensics determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.

Remediation

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Affected hosts

172.16.11.32, 172.16.11.30, 172.16.11.2, 172.16.11.31, 172.16.11.24, 172.16.11.23, 172.16.11.26

References
https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Vulnerability	Count	Severity
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	4	2

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

Output

EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

```
EXP-DES-CBC-SHA          Kx=RSA(512)   Au=RSA     Enc=DES-CBC(40)        Mac=SHA1   export
EXP-RC2-CBC-MD5          Kx=RSA(512)   Au=RSA     Enc=RC2-CBC(40)        Mac=MD5    export
EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)            Mac=MD5    export
```

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Remediation

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Affected hosts

172.16.11.30, 172.16.11.31, 172.16.11.2

References

https://www.smacktls.com/#freak
https://www.openssl.org/news/secadv/20150108.txt
http://www.nessus.org/u?b78da2c4

Vulnerability	Count	Severity
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	4	2

Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

Output

The remote host is affected by SSL DROWN and supports the following
vulnerable cipher suites :

Low Strength Ciphers (<= 64-bit key)

DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=MD5
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

High Strength Ciphers (>= 112-bit key)

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Remediation

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

Affected hosts

172.16.11.30, 172.16.11.31, 172.16.11.2

References

https://drownattack.com/
https://drownattack.com/drown-attack-paper.pdf

Vulnerability	Count	Severity
SSL Weak Cipher Suites Supported	4	2

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Output

Here is the list of weak SSL ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

```
DES-CBC-MD5              Kx=RSA      Au=RSA    Enc=DES-CBC(56)      Mac=MD5
EXP-RC2-CBC-MD5          Kx=RSA(512) Au=RSA    Enc=RC2-CBC(40)      Mac=MD5  export
EXP-RC4-MD5              Kx=RSA(512) Au=RSA    Enc=RC4(40)          Mac=MD5  export
RC4-64-MD5               Kx=RSA      Au=RSA    Enc=RC4(64)          Mac=MD5
EXP-EDH-RSA-DES-CBC-SHA  Kx=DH(512)  Au=RSA    Enc=DES-CBC(40)      Mac=SHA1 export
EDH-RSA-DES-CBC-SHA      Kx=DH       Au=RSA    Enc=DES-CBC(56)      Mac=SHA1
EXP-DES-CBC-SHA          Kx=RSA(512) Au=RSA    Enc=DES-CBC(40)      Mac=SHA1 export
EXP-RC2-CBC-MD5          Kx=RSA(512) Au=RSA    Enc=RC2-CBC(40)      Mac=MD5  export
EXP-RC4-MD5              Kx=RSA(512) Au=RSA    Enc=RC4(40)          Mac=MD5  export
DES-CBC-SHA              Kx=RSA      Au=RSA    Enc=DES-CBC(56)      Mac=SHA1
```

The fields above are :

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

Remediation

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Affected hosts

172.16.11.30, 172.16.11.31, 172.16.11.2

References

http://www.nessus.org/u?6527892d

Vulnerability	Count	Severity
OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	4	2

Description

The version of OpenSSL on the remote host has been shown to allow resuming session with a weaker cipher than was used when the session was initiated. This means that an attacker that sees (i.e., by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a weaker cipher chosen by the attacker.

Note that other SSL implementations may also be affected by this vulnerability.

Output

The server allowed the following session over TLSv1 to be resumed as follows :

```
Session ID     : acbd843f50cdb49c9e67ee8a87780b177afa472a0c0696be89357bfcd5ca4448
Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Resumed Cipher : TLS1_CK_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
```

Remediation

Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.

Affected hosts

172.16.11.30, 172.16.11.31, 172.16.11.2

References

https://www.openssl.org/news/secadv/20101202.txt

Vulnerability	Count	Severity
IP Forwarding Enabled	1	2

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Output

No output recorded

Remediation

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Affected hosts

172.16.11.2

References

Vulnerability	Count	Severity
OpenSSH < 4.3 scp Command Line Filename Processing Command Injection	1	2

Description

According to its banner, the version of OpenSSH running on the remote host is potentially affected by an arbitrary command execution vulnerability. The scp utility does not properly sanitize user-supplied input prior to using a system() function call. A local attacker could exploit this by creating filenames with shell metacharacters, which could cause arbitrary code to be executed if copied by a user running scp.

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 4.3

Remediation

Upgrade to OpenSSH 4.3 or later.

Affected hosts

172.16.11.2

References

https://bugzilla.mindrot.org/show_bug.cgi?id=1094
http://www.openssh.com/txt/release-4.3

Vulnerability	Count	Severity
OpenSSH < 4.9 'ForceCommand' Directive Bypass	1	2

Description

According to its banner, the version of OpenSSH installed on the remote host is earlier than 4.9. It may allow a remote, authenticated user to bypass the 'sshd_config' 'ForceCommand' directive by modifying the '.ssh/rc' session file.

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 4.9

Remediation

Upgrade to OpenSSH version 4.9 or later.

Affected hosts

172.16.11.2

References

https://www.openssh.com/txt/release-4.9

Vulnerability	Count	Severity
OpenSSH With OpenPAM DoS	1	2

Description

According to its banner, the version of OpenSSH running on the remote host is affected by a remote denial of service vulnerability. When used with OpenPAM, OpenSSH does not properly handle when a forked child process ends during PAM authentication. This could allow a remote attacker to cause a denial of service by connecting several times to the SSH server, waiting for the password prompt and then disconnecting.

Output

```
Version source    : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 3.8.1p1
```

Remediation

Upgrade to OpenSSH 3.8.1p1 or later.

Affected hosts

172.16.11.2

References

https://bugzilla.mindrot.org/show_bug.cgi?id=839
http://www.nessus.org/u?170f19e3

Vulnerability	Count	Severity
Portable OpenSSH < 3.8p1 Multiple Vulnerabilities	1	2

Description

According to its banner, a version of OpenSSH earlier than 3.8p1 is running on the remote host and is affected by the following issues:

- There is an issue in the handling of PAM modules in such versions of OpenSSH. As a result, OpenSSH may not correctly handle aborted conversations with PAM modules. Consequently, that memory may not be scrubbed of sensitive information such as credentials, which could lead to credentials leaking into swap space and core dumps. Other vulnerabilities in PAM modules could come to light because of unpredictable behavior.

- Denial of service attacks are possible when privilege separation is in use. This version of OpenSSH does not properly signal non-privileged processes after session termination when 'LoginGraceTime' is exceeded. This can allow connections to remain open thereby allowing the denial of service when resources are exhausted. (CVE-2004-2069)

Output

```
Version source    : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 3.8p1
```

Remediation

Upgrade to OpenSSH 3.8p1 or later.

Affected hosts

172.16.11.2

References

https://www.cl.cam.ac.uk/~mgk25/otpw.html#opensshbug
https://bugzilla.mindrot.org/show_bug.cgi?id=632
http://www.nessus.org/u?e86aec66
http://www.nessus.org/u?bbd79dfd
http://www.nessus.org/u?d2f25e5c

Vulnerability	Count	Severity
OpenSSH X11 Forwarding Session Hijacking	1	2

Description

According to its banner, the version of SSH installed on the remote host is older than 5.0. Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use.

Output

The remote OpenSSH server returned the following banner :

SSH-2.0-OpenSSH_2.9p2

Remediation

Upgrade to OpenSSH version 5.0 or later.

Affected hosts

172.16.11.2

References

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
https://www.openssh.com/txt/release-5.0

Vulnerability	Count	Severity
OpenSSH < 5.2 CBC Plaintext Disclosure	1	2

Description

The version of OpenSSH running on the remote host has an information disclosure vulnerability. A design flaw in the SSH specification could allow a man-in-the-middle attacker to recover up to 32 bits of plaintext from an SSH-protected connection in the standard configuration. An attacker could exploit this to gain access to sensitive information.

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 5.2

Remediation

Upgrade to OpenSSH 5.2 or later.

Affected hosts

172.16.11.2

References

http://www.nessus.org/u?4984aeb9
http://www.openssh.com/txt/cbc.adv
http://www.openssh.com/txt/release-5.2

Vulnerability	Count	Severity
OpenSSH < 3.0.1 Multiple Flaws	1	2

Description

According to its banner, the remote host appears to be running OpenSSH version 3.0.1 or older. Such versions are reportedly affected by multiple flaws :

- Provided KerberosV is enabled (disabled by default), it may be possible for an attacker to partially authenticate.

- It may be possible to crash the daemon due to a excessive memory clearing bug.

Output

No output recorded

Remediation

Upgrade to OpenSSH 3.0.1 or later.

Affected hosts

172.16.11.2

References

https://seclists.org/bugtraq/2001/Nov/152

Vulnerability	Count	Severity
SSL / TLS Certificate Known Hard Coded Private Keys	2	2

Description

The remote host is running a service that is using a publicly known SSL / TLS private key.
An attacker may use this key to decrypt intercepted traffic between users and the device.
A remote attacker can also perform a man-in-the-middle attack in order to gain access to the system or modify data in transit.

Output

- HTTPS certificate fingerprint : 69C90653B260357376FD66D3AADD1E41ABA863C2
HTTPS fingerprint type : SHA1

Reference : https://github.com/sec-consult/houseofkeys

Remediation

Where possible, change the X.509 certificates so that they are unique to the device or contact vendor for guidance.

Affected hosts

172.16.11.2

References

http://www.nessus.org/u?48f09948
https://github.com/sec-consult/houseofkeys
https://www.kb.cert.org/vuls/id/566724/

Vulnerability	Count	Severity
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	2	2

Description

The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake.
An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

Output

TLSv1 supports insecure renegotiation.

SSLv3 supports insecure renegotiation.

Remediation

Contact the vendor for specific patch information.

Affected hosts

172.16.11.2

References

http://www.ietf.org/mail-archive/web/tls/current/msg03948.html
http://www.g-sec.lu/practicaltls.pdf
https://tools.ietf.org/html/rfc5746

Vulnerability	Count	Severity
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	3	2

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

Output

Oxytis Forensics was able to negotiate non-NLA (Network Level Authentication) security.

Remediation

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Affected hosts

172.16.11.23, 172.16.11.32, 172.16.11.24

References

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)
http://www.nessus.org/u?e2628096

Vulnerability	Count	Severity
Terminal Services Encryption Level is Medium or Low	2	2

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Output

The terminal services encryption level is set to :

2. Medium

Remediation

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Affected hosts

172.16.11.32, 172.16.11.24

References

Vulnerability	Count	Severity
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	2	2

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Output

No output recorded

Remediation

- Force the use of SSL as a transport layer for this service if supported, or/and

- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Affected hosts

172.16.11.32, 172.16.11.24

References

http://www.oxid.it/downloads/rdp-gbu.pdf
http://www.nessus.org/u?8033da0d
http://technet.microsoft.com/en-us/library/cc782610.aspx

Vulnerability	Count	Severity
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	1	2

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Output

No output recorded

Remediation

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Affected hosts

172.16.11.24

References

http://www.nessus.org/u?52ade1e9
http://badlock.org/

Vulnerability	Count	Severity
SSL Certificate with Wrong Hostname	3	2

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Output

The identities known by Oxytis Forensics are :

172.16.11.24
172.16.11.24

The Common Name in the certificate is :

SSL_Self_Signed_Fallback

Remediation

Purchase or generate a proper certificate for this service.

Affected hosts

172.16.11.23, 172.16.11.31, 172.16.11.24

References

Vulnerability	Count	Severity
ESXi 5.0 < Build 1918656 OpenSSL Library Multiple Vulnerabilities (remote check)	1	2

Description

The remote VMware ESXi host is version 5.0 prior to build 1918656. It is, therefore, affected by the following vulnerabilities in the OpenSSL library :

- An error exists in the function 'ssl3_read_bytes' that could allow data to be injected into other sessions or allow denial of service attacks. Note this issue is only exploitable if 'SSL_MODE_RELEASE_BUFFERS' is enabled. (CVE-2010-5298)

- An error exists in the function 'do_ssl3_write' that could allow a NULL pointer to be dereferenced leading to denial of service attacks. Note this issue is exploitable only if 'SSL_MODE_RELEASE_BUFFERS' is enabled. (CVE-2014-0198)

- An unspecified error exists that could allow an attacker to cause usage of weak keying material leading to simplified man-in-the-middle attacks.
(CVE-2014-0224)

- An unspecified error exists related to anonymous ECDH ciphersuites that could allow denial of service attacks. Note this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

Output

ESXi version : ESXi 5.0
Installed build : 914586
Fixed build : 1918656

Remediation

Apply patch ESXi500-201407001 for ESXi 5.0.

Affected hosts

172.16.11.26

References

http://www.vmware.com/security/advisories/VMSA-2014-0006.html
http://www.nessus.org/u?c7cdd0f9
https://www.openssl.org/news/secadv/20140605.txt

Vulnerability	Count	Severity
ESXi 5.0 / 5.1 / 5.5 / 6.0 Multiple Vulnerabilities (VMSA-2016-0010) (remote check)	1	2

Description

The remote VMware ESXi host is version 5.0, 5.1, 5.5, or 6.0 and is missing a security patch. It is, therefore, affected by multiple vulnerabilities :

- An arbitrary code execution vulnerability exists in the Shared Folders (HGFS) feature due to improper loading of Dynamic-link library (DLL) files from insecure paths, including the current working directory, which may not be under user control. A remote attacker can exploit this vulnerability, by placing a malicious DLL in the path or by convincing a user into opening a file on a network share, to inject and execute arbitrary code in the context of the current user. (CVE-2016-5330)

- An HTTP header injection vulnerability exists due to improper sanitization of user-supplied input. A remote attacker can exploit this to inject arbitrary HTTP headers and conduct HTTP response splitting attacks. (CVE-2016-5331)

Output

ESXi version : 5.0
Installed build : 914586
Fixed build : 3982828 / 3982819 (security-only fix)

Remediation

Apply the appropriate patch as referenced in the vendor advisory.

Note that VMware Tools on Windows-based guests that use the Shared Folders (HGFS) feature must also be updated to completely mitigate CVE-2016-5330.

Affected hosts

172.16.11.26

References

http://www.vmware.com/security/advisories/VMSA-2016-0010.html
http://kb.vmware.com/kb/2142193
http://kb.vmware.com/kb/2143976
http://kb.vmware.com/kb/2141429
http://kb.vmware.com/kb/2144359

Vulnerability	Count	Severity
ESXi 5.0 < Build 1311175 Multiple Vulnerabilities (remote check)	1	2

Description

The remote VMware ESXi 5.0 host is affected by the following security vulnerabilities :

- Multiple errors exist related to OpenSSL that could allow information disclosure or denial of service attacks. (CVE-2013-0166, CVE-2013-0169)

- An error exists in the libxml2 library related to the expansion of XML internal entities. An attacker can exploit this to cause a denial of service. (CVE-2013-0338)

- An unspecified error exists related to 'hostd-vmdb'. An attacker can exploit this to cause a denial of service. (CVE-2013-5970)

- An error exists in the handling of certain Virtual Machine file descriptors. This may allow an unprivileged user with the 'Add Existing Disk' privilege to obtain read and write access to arbitrary files, possibly leading to arbitrary code execution after a host reboot. (CVE-2013-5973)

- A NULL pointer dereference flaw exists in the handling of Network File Copy (NFC) traffic. This issue may lead to a denial of service if an attacker intercepts and modifies the NFC traffic. (CVE-2014-1207)

- A denial of service vulnerability exists in the handling of invalid ports that could allow a guest user to crash the VMX process. (CVE-2014-1208)

Output

ESXi version : ESXi 5.0
Installed build : 914586
Fixed build : 1311175

Remediation

Apply patch ESXi500-201310101-SG, ESXi500-201310201-UG, or ESXi500-Update03.

Affected hosts

172.16.11.26

References

http://www.nessus.org/u?07980398
https://www.vmware.com/security/advisories/VMSA-2013-0009.html
https://www.vmware.com/security/advisories/VMSA-2013-0012.html
https://www.vmware.com/security/advisories/VMSA-2013-0016.html

https://www.vmware.com/security/advisories/VMSA-2014-0001.html

Vulnerability	Count	Severity
VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2014-0002)	1	2

Description

The remote VMware ESX / ESXi host is affected by multiple vulnerabilities :

- Multiple integer overflow conditions exist in the glibc package in file malloc/malloc.c. An unauthenticated, remote attacker can exploit these to cause heap memory corruption by passing large values to the pvalloc(), valloc(), posix_memalign(), memalign(), or aligned_alloc() functions, resulting in a denial of service. (CVE-2013-4332)

- A distributed denial of service (DDoS) vulnerability exists in the NTP daemon due to improper handling of the 'monlist' command. A remote attacker can exploit this, via a forged request to an affected NTP server, to cause an amplified response to the intended target of the DDoS attack. (CVE-2013-5211)

Output

Version : ESXi 5.0
Installed build : 914586
Fixed build : 1749766 / 1851670

Remediation

Apply the appropriate patch according to the vendor advisory that pertains to ESX version 4.0 / 4.1 and ESXi version 4.0 / 4.1 / 5.0 / 5.1 / 5.5.

Affected hosts

172.16.11.26

References

https://www.vmware.com/security/advisories/VMSA-2014-0002
http://lists.vmware.com/pipermail/security-announce/2014/000281.html

Vulnerability	Count	Severity
VMware ESX / ESXi Multiple DoS (VMSA-2014-0001)	1	2

Description

The remote VMware ESX / ESXi host is affected by multiple denial of service vulnerabilities :

- A denial of service vulnerability exists due to a NULL pointer deference flaw when handling Network File Copy (NFC) traffic. An unauthenticated, remote attacker can exploit this by intercepting and modifying the traffic between the ESX / ESXi host and the client.
(CVE-2014-1207)

- A flaw exists due to improper handling of invalid ports. An unauthenticated attacker on an adjacent network can exploit this to cause VMX processing to fail, resulting in a partial denial of service.
(CVE-2014-1208)

Output

Version : ESXi 5.0
Installed build : 914586
Fixed build : 1311175 / 1311177

Remediation

Apply the appropriate patch according to the vendor advisory that pertains to ESX version 4.0 / 4.1 and ESXi version 4.0 / 4.1 / 5.0 / 5.1.

Affected hosts

172.16.11.26

References

https://www.vmware.com/security/advisories/VMSA-2014-0001
http://lists.vmware.com/pipermail/security-announce/2014/000231.html

Vulnerability	Count	Severity
VMware ESXi Multiple OpenSSL Vulnerabilities (VMSA-2014-0006)	1	2

Description

The remote VMware ESXi host is affected by multiple vulnerabilities in the OpenSSL third-party library :

- A use-after-free error exists in the ssl3_read_bytes() function in file ssl/s3_pkt.c that is triggered when a second

read is done to the function by multiple threads when SSL_MODE_RELEASE_BUFFERS is enabled. A man-in-the-middle attacker can exploit this to dereference already freed memory and inject arbitrary data into the SSL stream. (CVE-2010-5298)

- A NULL pointer dereference flaw exists in the do_ssl3_write() function in file ssl/s3_pkt.c due to a failure to properly manage a buffer pointer during certain recursive calls when SSL_MODE_RELEASE_BUFFERS is enabled. A remote attacker can exploit this, by triggering an alert condition, to cause a denial of service. (CVE-2014-0198)

- A flaw exists due to a failure to properly restrict processing of ChangeCipherSpec messages. A man-in-the-middle attacker can exploit this, via a crafted TLS handshake, to force the use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, resulting in the session being hijacked and sensitive information being disclosed. (CVE-2014-0224)

- A NULL pointer dereference flaw exists in the ssl3_send_client_key_exchange() function in file s3_clnt.c, when an anonymous ECDH cipher suite is used, that allows a remote attacker to cause a denial of service. (CVE-2014-3470)

Output

Version : ESXi 5.0
Installed build : 914586
Fixed build : 1918656

Remediation

Apply the appropriate patch according to the vendor advisory that pertains to ESXi version 5.0 / 5.1 / 5.5.

Affected hosts

172.16.11.26

References

https://www.vmware.com/security/advisories/VMSA-2014-0006
http://lists.vmware.com/pipermail/security-announce/2014/000276.html

Vulnerability	Count	Severity
ESXi 5.0 < Build 1197855 NFC Traffic Denial of Service (remote check)	1	2

Description

The remote VMware ESXi 5.0 host is affected by an unspecified error related to handling Network File Copy (NFC) traffic that could allow denial of service attacks.

Output

ESXi version : ESXi 5.0
Installed build : 914586
Fixed build : 1197855

Remediation

Apply patch ESXi500-201308101-SG.

Affected hosts

172.16.11.26

References

http://www.nessus.org/u?6145a319
https://www.vmware.com/security/advisories/VMSA-2013-0011.html

Vulnerability	Count	Severity
ESXi 5.0 < Build 1749766 Multiple Vulnerabilities (remote check)	1	2

Description

The remote VMware ESXi host is version 5.0 prior to build 1749766. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists in the monlist feature in NTP. A remote attacker can exploit this flaw, using a specially crafted packet to load the query function in monlist, to conduct a distributed denial of service attack. (CVE-2013-5211)

- An unspecified privilege escalation vulnerability exists that allows an attacker to gain host OS privileges or cause a denial of service condition by modifying a configuration file. (CVE-2014-8370)

Output

ESXi version : ESXi 5.0
Installed build : 914586
Fixed build : 1749766

Remediation

Apply patch ESXi500-201405001 for ESXi 5.0.

Affected hosts

172.16.11.26

References

https://www.vmware.com/security/advisories/VMSA-2014-0002.html
https://www.vmware.com/security/advisories/VMSA-2015-0001.html
http://www.nessus.org/u?3054e515

Vulnerability	Count	Severity
ESXi 5.0 < Build 3086167 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)	1	2

Description

The remote VMware ESXi 5.0 host is prior to build 3086167. It is, therefore, affected by a guest privilege escalation vulnerability in the Shared Folders (HGFS) feature due to improper validation of user-supplied input. A local attacker can exploit this to corrupt memory, resulting in an elevation of privileges.

Output

ESXi version : ESXi 5.0
Installed build : 914586
Fixed build : 3086167

Remediation

Apply patch ESXi500-201510102-SG according to the vendor advisory.

Note that VMware Tools in any Windows-based guests that use the Shared Folders (HGFS) feature must also be updated to completely mitigate the vulnerability.

Affected hosts

172.16.11.26

References

http://www.vmware.com/security/advisories/VMSA-2016-0001.html
http://www.nessus.org/u?a70e58b8
http://www.nessus.org/u?98b39737

Vulnerability	Count	Severity
VMware ESXi Tools Guest OS Privilege Escalation (VMSA-2014-0005)	1	2

Description

The remote VMware ESXi host is affected by a privilege escalation vulnerability due to a NULL pointer dereference flaw in VMware Tools running on Microsoft Windows 8.1. An attacker on an adjacent network can exploit this issue to gain elevated privileges within the guest operating system or else cause the guest operating system to crash.

Output

Version : ESXi 5.0
Installed build : 914586
Fixed build : 1749766 / 1851670

Remediation

Apply the appropriate patch according to the vendor advisory that pertains to ESXi version 5.0 / 5.1 / 5.5.

Affected hosts

172.16.11.26

References

https://www.vmware.com/security/advisories/VMSA-2014-0005
http://lists.vmware.com/pipermail/security-announce/2014/000247.html

Low Findings

Vulnerability	Count	Severity
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	20	1

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Output

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

RC4-MD5	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=MD5
RC4-SHA	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Remediation

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Affected hosts

172.16.11.32, 172.16.11.30, 172.16.11.2, 172.16.11.153, 172.16.11.103, 172.16.11.154, 172.16.11.152, 172.16.11.108, 172.16.11.24, 172.16.11.105, 172.16.11.109, 172.16.11.23, 172.16.11.31, 172.16.11.151

References

http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Vulnerability	Count	Severity
SSH Weak MAC Algorithms Enabled	3	1

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Output

The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-sha1-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-sha1-96

Remediation

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Affected hosts

172.16.11.21, 172.16.11.30, 172.16.11.2

References

Vulnerability	Count	Severity
SSH Server CBC Mode Ciphers Enabled	3	1

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Output

The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Remediation

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Affected hosts

172.16.11.21, 172.16.11.30, 172.16.11.2

References

Vulnerability	Count	Severity
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	2	1

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

Output

EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Remediation

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Affected hosts

172.16.11.30, 172.16.11.31

References

https://weakdh.org/

Vulnerability	Count	Severity
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	7	1

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Output

Vulnerable connection combinations :

SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

Remediation

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Affected hosts

172.16.11.23, 172.16.11.32, 172.16.11.30, 172.16.11.31

References

https://weakdh.org/

Vulnerability	Count	Severity
OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking	1	1

Description

According to its banner, the version of SSH installed on the remote host is older than 5.1 and may allow a local user to hijack the X11 forwarding port. The application improperly sets the 'SO_REUSEADDR' socket option when the 'X11UseLocalhost' configuration option is disabled.

Note that most operating systems, when attempting to bind to a port that has previously been bound with the 'SO_REUSEADDR' option, will check that either the effective user-id matches the previous bind (common BSD-derived systems) or that the bind addresses do not overlap (Linux and Solaris). This is not the case with other operating systems such as HP-UX.

Output

Version source : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version : 5.1

Remediation

Upgrade to OpenSSH version 5.1 or later.

Affected hosts

172.16.11.2

References

https://www.openssh.com/txt/release-5.1

Vulnerability	Count	Severity
OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure	1	1

Description

According to its banner, the remote host is running a version of OpenSSH prior to 4.0. Versions of OpenSSH earlier than 4.0 are affected by an information disclosure vulnerability because the application stores hostnames, IP addresses, and keys in plaintext in the 'known_hosts' file. A local attacker, exploiting this flaw, could gain access to sensitive information that could be used in subsequent attacks.

Output

```
Version source    : SSH-2.0-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 4.0
```

Remediation

Upgrade to OpenSSH 4.0 or later.

Affected hosts

172.16.11.2

References

https://www.openssh.com/txt/release-4.0
http://nms.csail.mit.edu/projects/ssh/
http://www.eweek.com/c/a/Security/Researchers-Reveal-Holes-in-Grid/

Vulnerability	Count	Severity
OpenSSH < 4.2 Multiple Vulnerabilities	1	1

Description

According to its banner, the version of OpenSSH installed on the remote host has the following vulnerabilities :

- X11 forwarding may be enabled unintentionally when multiple forwarding requests are made on the same session, or when an X11 listener is orphaned after a session goes away. (CVE-2005-2797)

- GSSAPI credentials may be delegated to users who log in using something other than GSSAPI authentication if 'GSSAPIDelegateCredentials' is enabled. (CVE-2005-2798)

- Attempting to log in as a nonexistent user causes the authentication process to hang, which could be exploited to enumerate valid user accounts.
  Only OpenSSH on Mac OS X 10.4.x is affected.
  (CVE-2006-0393)

- Repeatedly attempting to log in as a nonexistent user could result in a denial of service.
  Only OpenSSH on Mac OS X 10.4.x is affected.
  (CVE-2006-0393)

Output

No output recorded

Remediation

Upgrade to OpenSSH 4.2 or later. For OpenSSH on Mac OS X 10.4.x, apply Mac OS X Security Update 2006-004.

Affected hosts

172.16.11.2

References

http://www.openssh.com/txt/release-4.2
https://lists.apple.com/archives/security-announce/2006/Aug/msg00000.html
https://support.apple.com/?artnum=304063

Vulnerability	Count	Severity
Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	1	1

Description

According to its banner, the version of OpenSSH running on the remote host is earlier than 5.8p2. Such versions may be affected by a local information disclosure vulnerability that could allow the contents of the host's private key to be accessible by locally tracing the execution of the ssh-keysign utility. Having the host's private key may allow the impersonation of the host.

Note that installations are only vulnerable if ssh-rand-helper was enabled during the build process, which is not the case for *BSD, OS X, Cygwin and Linux.

Output

```
Version source    : SSH-2.0-OpenSSH_2.9p2
```

Installed version : 2.9p2
Fixed version : 5.8p2

Remediation

Upgrade to Portable OpenSSH 5.8p2 or later.

Affected hosts

172.16.11.2

References

http://www.openssh.com/txt/portable-keysign-rand-helper.adv
http://www.openssh.com/txt/release-5.8p2

Vulnerability	Count	Severity
Terminal Services Encryption Level is not FIPS-140 Compliant	2	1

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Output

The terminal services encryption level is set to :

2. Medium (Client Compatible)

Remediation

Change RDP encryption level to :

4. FIPS Compliant

Affected hosts

172.16.11.32, 172.16.11.24

References

Vulnerability	Count	Severity
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	2	1

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Oxytis Forensics will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

Output

The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject : CN=SSL_Self_Signed_Fallback
|-RSA Key Length : 1024 bits

Remediation

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Affected hosts

172.16.11.23, 172.16.11.24

References

https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Vulnerability	Count	Severity
Transport Layer Security (TLS) Protocol CRIME Vulnerability	3	1

Description

The remote service has one of two configurations that are known to be required for the CRIME attack :

- SSL / TLS compression is enabled.

- TLS advertises the SPDY protocol earlier than version 4.

Note that Oxytis Forensics did not attempt to launch the CRIME attack against the remote service.

Output

The following configuration indicates that the remote service
may be vulnerable to the CRIME attack :

- SSL / TLS compression is enabled.

Remediation

Disable compression and / or the SPDY service.

Affected hosts

172.16.11.31, 172.16.11.26

References

https://www.iacr.org/cryptodb/data/paper.php?pubkey=3091
https://discussions.nessus.org/thread/5546
http://www.nessus.org/u?c44d5826
https://bz.apache.org/bugzilla/show_bug.cgi?id=53219

6.0 ASSESSMENT METHODOLOGY

Network Footprinting (Reconnaissance): Gather as much information as possible about the selected network. Reconnaissance can take two forms i.e. active and passive. A passive attack is always the best starting point as this would normally defeat intrusion detection systems and other forms of protection etc. afforded to the network. This would usually involve trying to discover publicly available information by utilizing a web browser and visiting newsgroups etc. An active form would be more intrusive and may show up in audit logs and may take the form of an attempted DNS zone transfer or a social engineering type of attack.

Discovery & Probing: Enumeration can serve two distinct purposes in an assessment: OS Fingerprinting Remote applications being served. OS fingerprinting or TCP/IP stack fingerprinting is the process of determining the operating system being utilized on a remote host. This is carried out by analyzing packets received from the host in question. There are two distinct ways to OS fingerprint, actively (i.e. nmap) or passively (i.e. scanrand). Passive OS fingerprinting determines the remote OS utilizing the packets received only and does not require any packets to be sent. Active OS fingerprinting is very noisy and requires packets to be sent to the remote host and waits for a reply, (or lack thereof). Disparate OSs respond differently to certain types of packet, (the response is governed by an RFC and any proprietary responses the vendor (notably Microsoft) has enabled within the system) and so custom packets may be sent. Remote applications being served on a host can be determined by an open port on that host. By port scanning it is then possible to build up a picture of what applications are running and tailor the test accordingly.

Vulnerability Assessment: Utilizing vulnerability scanners all discovered hosts can then be tested for vulnerabilities. The result would then be analyzed to determine if there any vulnerabilities that could be exploited to gain access to a target host on a network. A number of tests carried out by these scanners are just banner grabbing/ obtaining version information, once these details are known, the version is compared with any common vulnerabilities and exploits (CVE) that have been released and reported to the user. Other tools actually use manual pen testing methods and display the output received i.e. showmount -e ip_address would display the NFS shares available to the scanner which would then need to be verified by the tester.

Forensic Assessment: Delivers only relevant vulnerabilities and those with exploits or having exploitable conditions typically attempted during a penetration test. Additionally, this assessment derives a unique threat model from the assessment data to discover possible misuse, potentially unwanted programs and backdoors in the environment. Essential for post breach assessments, discovery of protocol misuse, blacklisted IPs and those on blocklists by malware, suspicious domains, safe browser checks, DGA typically used by malware, unusual traffic, geographic irregularities, remote access misuse, and various other telemetry are provided to discover indicators of compromise typically not found in traditional vulnerability assessment or penetration test.

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVEs common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

OWASP: The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. https://www.owasp.org/index.php/Top_10-2017_Top_10

PTES: Defines baseline methods that have been used in the industry covering everything related to a penetration test - from the initial communication and reasoning behind a pentest to reporting.

4/Critical
Description
A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs without warnings or prompts. This could mean browsing to a web page or opening email. Apply Critical updates immediately.
3/High
Description
XSS and other client-side attacks, extremely significant information disclosure (e.g. administrator hashes) Significant information disclosure, PII, user passwords. Valuable information disclosure (e.g. DNS zone transfers, account enumeration)
2/Medium
Description
A vulnerability which is known to lead to the compromise of the application or system being tested, however a mitigating factor is present. A vulnerability which may lead to compromise of the application or system being tested, however several mitigating factors are present (e.g. network configuration prevents talking directly to the required port) or exploitation is possible but only theoretical.
1/Low
Description
Other application or system specific information disclosure which does not fit (e.g. development notes, configuration files) Minor information disclosure, OS, patch levels (if current), etc. Non exploitable vulnerabilities which should still be addressed or low value information disclosure.