Network Ten

Cisco Report

June 2022

purple.telstra.com

Document Development

**Preparation**

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Name | Role | Date |
| Prepared By: | Chris Larkin | Technical Consultant | 1th July 2022 |
| Reviewed By: | Daniel Gonzalez | Technical Consultant | 11th July 2022 |

**Contact Details**

|  |  |
| --- | --- |
| Account Manager | |
| Name: | Nick Goodey |
| Phone: | +61 2 85761680 |
| Email: | Nick.Goodey@team.telstra.com |

**Distribution List**

|  |  |  |
| --- | --- | --- |
| Name | Title | Organisation |
| Costa Varvarigos | Communications Manager - Technology | Network Ten |

Table of Contents

[1 Executive Summary 4](#_Toc106280969)

[2 Incidents and Service Requests 5](#_Toc106280970)

[3 Firmware and Uptime Status 6](#_Toc106280971)

[3.1 Uptime 6](#_Toc106280972)

[3.2 Latest Firmware Revisions 7](#_Toc106280973)

[3.2.1 2900 and 3900 series routers 7](#_Toc106280974)

[3.2.2 ASR 1001-X 7](#_Toc106280975)

[3.3 Known critical Vulnerabilities 7](#_Toc106280976)

[4 Hardware EOL/EOS 7](#_Toc106280977)

[5 Recommendations 8](#_Toc106280978)

[6 Hardware Status 9](#_Toc106280979)

[6.1 Temperature Status 9](#_Toc106280980)

[6.2 Power Supply Status 10](#_Toc106280981)

[6.3 Fan Status 10](#_Toc106280982)

[7 Statistics 11](#_Toc106280983)

[7.1 ndw-ten-r01 11](#_Toc106280984)

[7.1.1 Interfaces 12](#_Toc106280985)

[7.2 ndw-ten-r02 14](#_Toc106280986)

[7.2.1 Interfaces 15](#_Toc106280987)

[7.3 ndw-atv-r01 17](#_Toc106280988)

[7.3.1 Interfaces 18](#_Toc106280989)

[7.4 ndw-atv-r02 20](#_Toc106280990)

[7.4.1 Interfaces 21](#_Toc106280991)

# Executive Summary

This report covers the availability and performance of the Cisco routers and switches within the Network Tenenvironment.

The report is summarized in the following dashboard.

|  |  |  |
| --- | --- | --- |
| Category | Comments | Status |
| Tickets | 7 Total: 7 Incidents + 0 Service Requests 0 Open, 7 Completed, 0 Cancelled | C:\InhouseApps\o2lib\Images\24x24\Tick.png |
| Firmware Status | There is newer firmware available, but there is no specific requirement to upgrade. | C:\InhouseApps\o2lib\Images\24x24\Tick.png |
| Uptime | No devices rebooted | C:\Users\robert.gruener\Downloads\1389264091_configure.png |
| Recommendations | No recommendations. | C:\InhouseApps\o2lib\Images\24x24\Tick.png |

|  |  |
| --- | --- |
| Symbol | Description |
| C:\InhouseApps\o2lib\Images\24x24\Tick.png | No issues of concern. |
|  | There are issues to be noted. |
| C:\Users\robert.gruener\Downloads\1389264091_configure.png | Work is required. |
| C:\InhouseApps\o2lib\Images\24x24\Exclamation.png | Important problems need to be fixed. |

# 

# Firmware and Uptime Status

Uptimes calculated on Friday, 1 July 2022

| **Name** | **Site** | **State** | **Address** | **Model** | **Serial Number** | **Firmware** | **Up Days** | **Status** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ndw-tvq-r01 | Brisbane Studio | QLD | 172.20.200.201 | ISR G2 3945E | FGL190511LH | 15.4(1)T3 | 2652 |  |
| ndw-tvq-r02 | Brisbane Studio | QLD | 172.20.200.202 | ISR G2 3945E | FGL190511LJ | 15.4(1)T3 | 2651 |  |
| ndw-gct-r01 | Gold Coast News Bureau | QLD | 172.20.200.205 | ISR 2921 | FGL190510RT | 15.3(3)M4 | 303 |  |
| ndw-gct-r02 | Gold Coast News Bureau | QLD | 172.20.200.206 | ISR 2921 | FGL190510Q0 | 15.3(3)M4 | 303 |  |
| ndw-atv-r01 | Melbourne Studio | VIC | 172.20.200.195 | ASR 1001-X | FXS1852Q1CC | 15.4(2r)S | 2571 |  |
| ndw-atv-r02 | Melbourne Studio | VIC | 172.20.200.196 | ASR 1001-X | FXS1847Q1Y1 | 15.4(2r)S | 2571 |  |
| txa-nws-r01 | Mt Lofty | SA | 172.20.200.213 | ISR 2901 | FGL190524WY | 15.4(3)M1 | 1115 |  |
| txa-crf-r01 | Mt Lofty (ex ADS/SAS) | SA | 172.20.200.211 | ISR 2901 | FGL190524WV | 15.4(3)M1 | 2662 |  |
| ndw-can-r01 | Parliament House | ACT | 172.20.200.203 | ISR 2921 | FTX1848AKM2 | 15.3(3)M4 | 159 |  |
| ndw-can-r02 | Parliament House | ACT | 172.20.200.204 | ISR 2921 | FGL190510Q1 | 15.3(3)M4 | 159 |  |
| ndw-new-r01 | Perth Studio | WA | 172.20.200.199 | ISR G2 3945E | FGL151111QA | 15.4(1)T3 | 101 |  |
| ndw-new-r02 | Perth Studio | WA | 172.20.200.200 | ISR G2 3945E | FGL190511KB | 15.4(1)T3 | 101 |  |
| ndw-ten-r01 | Sydney Studio | NSW | 172.20.200.193 | ASR 1001-X | FXS1852Q1FJ | 15.4(2r)S | 2569 |  |
| ndw-ten-r02 | Sydney Studio | NSW | 172.20.200.194 | ASR 1001-X | FXS1851Q1SG | 15.4(2r)S | 2569 |  |
| txa-art-r01 | TXA Artamon | NSW | 172.20.200.207 | ISR 2901 | FGL190524X2 | 15.4(3)M1 | 1428 |  |
| txa-bky-r01 | TXA Bickley | WA | 172.20.200.209 | ISR 2901 | FGL190524X1 | 15.4(3)M1 | 2520 |  |
| txa-cml-r01 | TXA Carmel | WA | 172.20.200.210 | ISR 2901 | FGL190524X0 | 15.4(3)M1 | 1709 |  |
| txa-eyr-r01 | TXA Mt Dandenong Backup | VIC | 172.20.200.212 | ISR 2901 | FGL190524X3 | 15.4(3)M1 | 2438 |  |
| txa-ota-r01 | TXA Mt Dandenong Primary | VIC | 172.20.200.214 | ISR 2901 | FGL190524WW | 15.4(3)M1 | 1247 |  |

## Uptime

No devices rebooted

## Latest Firmware Revisions

### 2900 and 3900 series routers

<https://software.cisco.com/download/home/282774229/type/280805680/>

<https://software.cisco.com/download/home/282774228/type/280805680/>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stream | Currently Installed Version | Suggested version | Latest Version | Release Date |
| **15.3M** | 15.3(3)M4 |  | 15.3.3M10(MD) | 31 Jul 2017 |
| **15.4T** | 15.4(1)T3 |  | 15.4.2T4(ED) | 15 Oct 2015 |
| **15.4M** | 15.4(3)M1 |  | 15.4.3M10(MD) | 10 Aug 2018 |
| **15.6M** |  | **15.6.3M9(MD)** | 15.6.3M9(MD) | 21 Sep 2020 |
| **15.7M** |  | **15.7.3M8(MD)** | 15.7.3M8(MD) | 09 Mar 2021 |

### ASR 1001-X

<https://software.cisco.com/download/home/284932298/type/282046477/release>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stream | Currently Installed Version | Suggested version | Latest Version | Release Date |
| **3.13** | 3.13.2S |  | 3.13.9S(MD) | 17 Mar 2018 |
| **16.6** |  |  | 16.6.9(MD) | 26 Feb 2021 |
| **16.12** |  | **16.12.5(MD)** | 16.12.7(MD) | 03 Feb 2022 |
| **17.3** |  | **17.3.5(MD)** | 17.3.5(MD) | 10 Feb 2022 |

## Known critical Vulnerabilities

There are known relevant critical vulnerabilities with the installed firmware.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cisco IOS Software Release | Advisory ID | Security Advisories | Publication Date | First Fixed |
| 15.3(3)M4  15.4(1)T3  15.4(3)M1  3.13.2S | CVE-2015-6280 | [Cisco IOS and IOS XE Software SSH Version 2 RSA-Based User Authentication Bypass Vulnerability](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-sshpk) | 2015 Sep 23 | 15.3(3)M10  15.5(3)M6  15.6(3)M2a  3.16.10S(MD) |
| 15.3(3)M4  15.4(1)T3  15.4(3)M1 | CVE-2017-12240 | [Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-dhcp) | 2017 Sep 27 | 15.3(3)M10  15.5(3)M6  15.6(3)M2a |
| 3.13.2S | CVE-2019-12643 | [Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass) | 2019 Aug 28 | 3.16.10S(MD) |

## Aruba

<Aruba>

## F5

<F5\_t1>

<F5\_t2>

<F5\_t3>

## Fortiguard

<Fortiguard>

## CISCO

<Cisco>

## Azure

<Azure>

<Azure\_CV>

<charts>

# Hardware EOL/EOS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Product | End Of Life | End of SW Maintenance | End of Service Contract Renewal | End Of Support | Link |
| 2900 and 3900 series | September 9, 2016 | December 9, 2020 | March 9, 2022 | December 31, 2022 | [Info Link](https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/eos-eol-notice-c51-737831.html) |
| ASR 1001-X | January 31, 2022 | August 1, 2023 | October 27, 2024 | July 31, 2027 | [Info Link](https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/asr1001-x-1002-x-eol.html) |

# Recommendations

For the critical vulnerabilities:

* CVE-2015-6280: Devices running a vulnerable version of Cisco IOS and Cisco IOS XE Software are affected if SSHv2 access is configured with RSA-based user authentication and at least one user is configured with a public key.

**Option not configured on devices, not affected.**

* CVE-2017-12240: This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS Software or Cisco IOS XE Software and are configured as a DHCP relay agent.

**Devices are not configured as DHCP agent**, **not affected.**

* CVE-2019-12643: This vulnerability affects Cisco devices that are configured to use a vulnerable version of Cisco REST API virtual service container.

**Option not configured on devices, not affected.**