America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Moxa NPort Device Vulnerabilities (Update A)

Last Revised: March 21, 2017 **Alert Code:** ICSA-16-336-02A

OVERVIEW

This updated advisory is a follow-up to the original advisory titled ICSA-16-336-02 Moxa NPort Device Vulnerabilities that was published December 1, 2016, on the NCCIC/ICS-CERT web site.

Security researchers Reid Wightman of RevICS Security, Mikael Vingaard, and Maxim Rupp have identified vulnerabilities in Moxa's NPort serial device servers. Moxa has produced new firmware versions to mitigate these vulnerabilities.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

--------- Begin Update A Part 1 of 2 --------

Moxa reports that the vulnerability affects the following versions of NPort:

- NPort 5110 versions prior to 2.7,
- NPort 5130/5150 Series versions prior to 3.7,
- NPort 5200 Series versions prior to 2.9,
- NPort 5400 Series versions prior to 3.12,
- NPort 5600 Series versions prior to 3.8,
- NPort 5100A Series & NPort P5150A versions prior to 1.4,
- NPort 5200A Series versions prior to 1.4,
- NPort 5150AI-M12 Series versions prior to 1.3,
- NPort 5250AI-M12 Series versions prior to 1.3,
- NPort 5450AI-M12 Series versions prior to 1.3,
- NPort 5600-8-DT Series versions prior to 2.5,
- NPort 5600-8-DTL Series versions prior to 2.5,
- NPort IA5450A versions prior to v1.4,
- NPort 6000 series versions prior to 1.16, and
- NPort 6110 series all versions

--------- End Update A Part 1 of 2 ----------

IMPACT

Successful exploitation of these vulnerabilities could lead to the complete compromise of an affected system.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Moxa is a Taiwan-based company that maintains offices in several countries around the world, including the US, UK, India, Germany, France, China, Russia, and Brazil.

The affected products, NPort devices, connect serial devices to Ethernet networks. According to Moxa, NPort devices are deployed across several sectors including Critical Manufacturing, Energy, and Transportation Systems. Moxa estimates that these products are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CREDENTIALS MANAGEMENTCWE-255: Credentials Management, http://cwe.mitre.org/data/definitions/255.html, web site last accessed December 01, 2016.

Administration passwords can be retried without authenticating.

CVE-2016-9361NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9361, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, web site last accessed December 01, 2016.

PERMISSIONS, PRIVILEGES, AND ACCESS CONTROLSCWE-264: Permissions, Privileges, and Access Controls, http://cwe.mitre.org/data/definitions/264.html, web site last accessed December 01, 2016.

Firmware can be updated over the network without authentication, which may allow remote code execution.

CVE-2016-9369NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9369, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, web site last accessed December 01, 2016.

CLASSIC BUFFER OVERFLOWCWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), http://cwe.mitre.org/data/definitions/120.html, web site last accessed December 01, 2016.

Buffer overflow vulnerability may allow an unauthenticated attacker to remotely execute arbitrary code.

CVE-2016-9363NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9363, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 7.3 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L, web site last accessed December 01, 2016.

CROSS-SITE SCRIPTINGCWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), http://cwe.mitre.org/data/definitions/79.html, web site last accessed December 01, 2016.

User-controlled input is not neutralized before being output to web page.

CVE-2016-9371NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9371, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 6.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N, web site last accessed December 01, 2016.

CROSS-SITE REQUEST FORGERYCWE-352: Cross-Site Request Forgery (CSRF), http://cwe.mitre.org/data/definitions/352.html, web site last accessed December 01, 2016.

Requests are not verified to be intentionally submitted by the proper user.

CVE-2016-9365NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9365, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H, web site last accessed December 01, 2016.

IMPROPER RESTRICTION OF EXCESSIVE AUTHENTICATION ATTEMPTSCWE-307: Improper Restriction of Excessive Authentication Attempts, http://cwe.mitre.org/data/definitions/307.html, web site last accessed December 01, 2016.

An attacker can freely use brute force to determine parameters needed to bypass authentication.

CVE-2016-9366NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9366, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, web site last accessed December 01, 2016.

PLAIN TEXT STORAGE OF A PASSWORDCWE-256: Plain Text Storage of a Password, http://cwe.mitre.org/data/definitions/256.html, web site last accessed December 01, 2016.

A configuration file contains parameters that represent passwords in plaintext.

CVE-2016-9348NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9348, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 3.3 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N, web site last accessed December 01, 2016.

RESOURCE EXHAUSTIONCWE-400: Uncontrolled Resource Consumption (‘Resource Exhaustion’), http://cwe.mitre.org/data/definitions/400.html, web site last accessed December 01, 2016.

The amount of resources requested by a malicious actor is not restricted, leading to a denial-of-service caused by resource exhaustion.

CVE-2016-9367NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9367, web site last accessed March 21, 2017. has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is

(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H, web site last accessed December 01, 2016.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with low skill would be able to exploit these vulnerabilities.

MITIGATION

--------- Begin Update A Part 2 of 2 --------

Moxa has released new firmware versions, which address the identified vulnerabilities in all but one of the affected NPort devices. Moxa recommends installing the new firmware version.

- NPort 5110 Version 2.7:

http://www.moxa.com/support/download.aspx?type=support&id=882

- NPort 5130/5150 Series Version 3.7:

http://www.moxa.com/support/download.aspx?type=support&id=356

- NPort 5200 Series Version 2.9:

http://www.moxa.com/support/download.aspx?type=support&id=904

- NPort 5400 Series Version 3.12:

http://www.moxa.com/support/download.aspx?type=support&id=925

- NPort 5600 Series Version 3.8:

http://www.moxa.com/support/download.aspx?type=support&id=905

- NPort 5100A Series & NPort P5150A Version 1.4:

http://www.moxa.com/support/download.aspx?type=support&id=1403

- NPort 5200A Series Version 1.4:

http://www.moxa.com/support/download.aspx?type=support&id=1462

- NPort 5150AI-M12 Series Version 1.3:

http://www.moxa.com/support/download.aspx?type=support&id=2206

- NPort 5250AI-M12 Series Version 1.3:

http://www.moxa.com/support/download.aspx?type=support&id=2207

- NPort 5450AI-M12 Series Version 1.3:

http://www.moxa.com/support/download.aspx?type=support&id=2208

- NPort 5600-8-DT Series Version 2.5:

http://www.moxa.com/support/download.aspx?type=support&id=938

- NPort 5600-8-DTL Series Version 1.4:

http://www.moxa.com/support/download.aspx?type=support&id=1819

- NPort IA5450A Version 1.4:

http://www.moxa.com/support/download.aspx?type=support&id=1469

- NPort 6000 Series Version 1.16:

http://www.moxa.com/support/download.aspx?type=support&id=733

--------- End Update A Part 2 of 2 ----------

Moxa has reported that the NPort 6110 device was discontinued in December 2008 and will not have patches released to address these vulnerabilities. Moxa recommends that customers using the NPort 6110 should upgrade the affected device.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Ensure that Ports 161/UDP, 4800/UDP, and 4900/TCP are only accessible by trusted systems and that restricting access to Ports 4800/UDP and 4900/TCP will impact remote systems administration.
- Ensure that all unused ports are disabled.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

ICS-CERT also provides a section for control systems security recommended practices </ics/content/recommended-practices> on the ICS-CERT web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>, that is available for download from the ICS-CERT web site </ics/>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

Vendor

- Moxa

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov