Advisory (ICSA-16-343-01)

Moxa MiiNePort Session Hijack Vulnerabilities

Original release date: December 08, 2016

OVERVIEW

Independent researcher Aditya Sood has identified vulnerabilities in Moxa's MiiNePort. Moxa has produced new firmware editions to mitigate these vulnerabilities.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

Moxa reports that the vulnerabilities affect the following versions of MiiNePort:

- MiiNePort E1 versions prior to 1.8,
- MiiNePort E2 versions prior to 1.4, and
- MiiNePort E3 versions prior to 1.1

IMPACT

An attacker may be able to gain user-level access to the target system by exploiting these vulnerabilities.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/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, the UK, India, Germany, France, China, Russia, and Brazil.

The affected product, MiiNePort, is a serial device server module. According to Moxa, MiiNePort is deployed across several sectors including Commercial Facilities, Critical Manufacturing, Energy, and Transportation Systems. Moxa estimates that this product is used primarily in the United States and Europe with a small percentage in Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

PERMISSIONS, PRIVILEGES, AND ACCESS CONTROLS[a]

An attacker may be able to brute force an active session cookie to be able to download configuration files.

CVE-2016-9344[b] has been assigned to this vulnerability. A CVSS v3 base score of 5.3 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).[c]

CLEARTEXT STORAGE OF SENSITIVE INFORMATION[d]

Configuration data are stored in a file that is not encrypted.

CVE-2016-9346[e] has been assigned to this vulnerability. A CVSS v3 base score of 5.3 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).[f]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

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

MITIGATION

Moxa has released new firmware editions, which address the identified vulnerabilities in MiiNePort devices. Moxa recommends installing these new firmware editions:

- MiiNePort E1 Series, Edition 1.8 http://www.moxa.com/support/download.aspx?type=support&id=1214
- MiiNePort E2 Series, Edition 1.4 http://www.moxa.com/support/download.aspx?type=support&id=263

- MiiNePort E3 Series, Edition 1.1 http://www.moxa.com/support/download.aspx?type=support&id=2058

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

- 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 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.

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, that is available for download from the ICS-CERT web site.

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.

---

a. CWE-264: Permissions, Privileges, and Access Controls, https://cwe.mitre.org/data/definitions/264.html, web site last accessed December 08, 2016.

b. NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9344, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory

c. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S..., web site last accessed December 08, 2016.

d. CWE-312: Cleartext Storage of Sensitive Information, https://cwe.mitre.org/data/definitions/312.html, web site last accessed December 08, 2016.

e. NVD, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9346, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory

f. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S..., web site last accessed December 08, 2016.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.