ICS-CERT ADVISORY

ICSA-13-042-01—MOXA EDR-G903 SERIES MULTIPLE VULNERABILITIES

February 11, 2013

OVERVIEW

This advisory provides mitigation details for vulnerabilities that impact Moxa EDR-G903 Series Routers.

Independent researcher Neil Smith identified a hard-coded user account vulnerability and an insufficient entropy vulnerability in Moxa's EDR-G903 series routers. By impersonating the device, an attacker can perform a Man-in-the-Middle (MitM) attack to obtain the credentials of administrative users. Moxa has produced and released a patch that resolves these vulnerabilities on December 17, 2012. Neil Smith has tested the patch and confirms that it fully resolves these vulnerabilities. If exploited, attackers could affect the availability, integrity, and confidentiality of the EDR-G903 routers. These vulnerabilities affect devices deployed in the critical manufacturing, commercial facilities, energy, water and wastewater, and other sectors.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following Moxa products are affected:

- EDR-G903 series routers, all versions.

IMPACT

An attacker can gain unauthorized access to the router by determining the authentication keys from reused or nonunique SSH and SSL host keys. Exploitation of this vulnerability would allow an attacker to perform a MitM attack and affect the integrity of the data on the 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, and Brazil. The EDR-G903 series routers are designed for networking industrial devices over media such as cellular networks, Ethernet, and more. According to Moxa, these routers are deployed across several sectors, including agriculture and food, critical manufacturing, government facilities, commercial facilities, chemical, emergency services, water and wastewater, and energy. Moxa estimates that these products are used globally but concentrated in the US, Europe, Chile, Argentina, Peru, Columbia, and Taiwan, with 50 to 60 percent of all sales in the US.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

HARD-CODED ACCOUNT[a]

The EDR-G903 series router had a hard-coded user account and password. According to Moxa, this account did not have any access rights to the router and was just an old account that had not been removed from the firmware. Successful exploitation of this vulnerability would allow an attacker to gain access to the router but not be able to make changes to configuration or traverse the network.

CVE-2012-4712[b] has been assigned to this vulnerability. A CVSS v2 base score of 4.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:P/I:N/A:N).[c]

INSUFFICIENT ENTROPY[d]

The EDR-G903 series router does not use sufficient entropy when generating keys for SSH and SSL connections; therefore, it makes these keys vulnerable to exploits. By calculating private authentication keys, an attacker could perform a MitM attack on the system by knowing the nonunique host key. This could enable the attacker to gain unauthorized access to the system and

a. CWE-259, http://cwe.mitre.org/data/definitions/259.html, CWE-259: Hard-Coded Password, Web site last accessed February 11, 2013.
b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4712, 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, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:P/I:N/A:N), Web site last visited February 11, 2013.
d. CWE-331, http://cwe.mitre.org/data/definitions/331.html, CWE-331: Insufficient Entropy, Web site last accessed February 11, 2013.

read information on the device, as well as send commands to the device, which would compromise the integrity of the data and could compromise the availability.

CVE-2012-4694[e] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[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 to high skill level would be able to exploit these vulnerabilities.

MITIGATION

Moxa has released customer notification and a firmware update (Moxa EDR-G903 Series Version 2.11) for this product. This update can be downloaded from the Moxa software download page.[g] This updated firmware fixes the vulnerabilities by replacing the hard-coded SSH/SSL key with dynamically-generated keys and adding support for special characters in login passwords.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face 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 VPN is only as secure as the connected devices.

e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4694, 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, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:H/Au:N/C:C/I:C/A:C), Web site last visited February 11, 2013.

g. Moxa Download Page, http://www.moxa.com/support/download.aspx?type=support&id=492, Web site last accessed February 11, 2013.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[h] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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,[i] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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.

ICS-CERT CONTACT

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed February 11, 2013.

i. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed February 11, 2013.

development of proper mitigations may put industrial control systems and the public at avoidable risk.