ICS-CERT ADVISORY

ICSA-12-146-01**A**—RUGGEDCOM WEAK CRYPTOGRAPHY FOR PASSWORD VULNERABILITY

UPDATE A

June 18, 2012

OVERVIEW

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

This is an update to the original advisory titled ICSA-12-146-01—RuggedCom Weak Cryptography for Password Vulnerability that was published May 25, 2012, on the ICS-CERT Web page. Independent researcher Justin W. Clarke identified a default backdoor user account[a,b,c] with a weak password encryption vulnerability in the RuggedCom Rugged Operating System (ROS). This vulnerability can be remotely exploited. Exploits that target this vulnerability are known to be publicly available.

Mr. Clarke provided this information to both CERT/CC and ICS-CERT. ICS-CERT coordinated a mitigation strategy with RuggedCom, a Siemens company. RuggedCom has produced new firmware versions that resolve the reported vulnerability.

Previous versions of this document erroneously stated that ICS-CERT had confirmed that the patch resolves the vulnerability. ICS-CERT has tested one version of the patched firmware (v3.10.1) and can confirm that the public exploits no longer work on the patched versions.

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

a. RuggedCom Backdoor Accounts, http://seclists.org/fulldisclosure/2012/Apr/277, Web site last accessed June 18, 2012.
b. US-CERT Vulnerability Note, http://www.kb.cert.org/vuls/id/889195, Web site last accessed June 18, 2012.
c. NERC Advisory, http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2012-05-07-01_Ruggedcom_Unauthorized_Access_Vulnerability.pdf, Web site last accessed June 18, 2012.

AFFECTED PRODUCTS

RuggedCom RuggedSwitch or RuggedServer devices are affected using the following versions of ROS:

- 3.2.x and earlier, and
- 3.3.x and above.

IMPACT

An attacker can use a simple publicly available script to generate the default password and gain administrative access to the unit.

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

BACKGROUND

RuggedCom makes network equipment that is intended for deployment in harsh environments. Their products can be found in applications such as traffic control systems, railroad communications systems, power plants, electrical substations, and military sites. Beyond Layer 2 and Layer 3 networking, these devices also provide serial-to-IP conversion in SCADA systems, and they support MODBUS and DNP3 protocols.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

WEAK CRYPTOGRAPHY FOR PASSWORDS[d]

An undocumented backdoor account exists within all previously released versions of RuggedCom's ROS. The username for the account, which cannot be disabled, is "factory," and its password is dynamically generated based on the device's MAC address.

CVE-2012-1803[e] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:S/C:C/I:C/A:C).[f]

d. CWE, http://cwe.mitre.org/data/definitions/261.html, Web site last accessed June 18, 2012.
e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1803, Web site last accessed June 18, 2012.
f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:S/C:C/I:C/A:C), Web site last visited June 18, 2012.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable remotely.

EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

DIFFICULTY

An attacker with a low skill level would be able to exploit this vulnerability.

MITIGATION

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

Versions 3.10.1, 3.9.3, 3.8.5, and 3.7.9 of the ROS firmware with security-related fixes are now available and can be obtained from RuggedCom technical support at support@ruggedcom.com.

ROS v3.11.x, a new firmware release containing additional functionality as well as the same security fixes, will be released within the next few weeks; RuggedCom will release a product bulletin[g] to notify customers when it is available.

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

To address security issues, the following changes are included in all the new ROS firmware versions:

- removal of factory account as referenced in ICSA -12-146-01 and NERC Alert A-2012-05-07-01,
- change default condition of insecure communication services to disabled,
- improval of security for user account password storage,
- detection and alarm for weak password strength, and
- removal of device information from standard login banner.

Note: These new versions of the ROS firmware remove the factory account and the associated security vulnerability. Customers using these new versions of the firmware should take special care not to lose the user defined password to a device's administrative account as recovering

g. Latest news on ROS Device Security Issue, http://www.ruggedcom.com/productbulletin/ros-security-page/, Web site last accessed June 18, 2012.

from a lost administrative password will now require physical access to the device to reset the passwords.

RuggedCom recommends that customers using ROS versions older than v3.7 upgrade to a newer version. If this is not possible, RuggedCom has indicated that they will address updates to older versions of the firmware on a case-by-case basis.

Siemens has issued security advisory "SSA-826381: Multiple Security Vulnerabilities in RuggedCom ROS-based Devices" regarding this vulnerability. It can be found on the Siemens ProductCERT advisory Web page.[h]

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.

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

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@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

h.Siemens ProductCERT advisories, http://www.siemens.com/cert/advisories/, Web site last accessed June 18, 2012.
i. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 18, 2012.

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