ICS-CERT ADVISORY

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

May 25, 2012

OVERVIEW

This advisory is a follow-up to the alert titled ICS-ALERT-12-116-01A—RuggedCom Weak Cryptography for Password Vulnerability that was published April 27, 2012, on the ICS-CERT web page.

Independent researcher Justin W. Clarke identified a default backdoor user account[abc] with a weak password encryption vulnerability in the RuggedCom Rugged Operating System (ROS). RuggedCom has produced new firmware versions that resolve the reported vulnerability. ICS-CERT has tested the new versions to confirm that they resolve the vulnerability. This vulnerability could be remotely exploited. Exploits that target this vulnerability are known to be publicly available.

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

a RuggedCom Backdoor Accounts, http://seclists.org/fulldisclosure/2012/Apr/277, Web site last accessed May 25, 2012

b US-CERT Vulnerability Note, http://www.kb.cert.org/vuls/id/889195, Web site last accessed May 25, 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 May 25, 2012.

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 are also used for serial-to-ip conversation 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 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]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable remotely.

EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

d. CWE, http://cwe.mitre.org/data/definitions/261.html, Web site last accessed May 25, 2012.
e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1803, Web site last accessed May 25, 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 May 25, 2012.

DIFFICULTY

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

MITIGATION

Version 3.10.1 of the ROS firmware with security-related fixes is now available and can be obtained from RuggedCom technical support at support@ruggedcom.com. Other ROS firmware versions containing the same security fixes (3.9.3, 3.8.5, 3.7.9, and 3.11.0) will be released over the next few weeks on a staggered basis as development and testing is completed.[g] RuggedCom will release a product bulletin to notify customers when each of the new versions is available.

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

- removal of factory account as referenced in ICS-ALERT-12-116-01A and NERC Alert A-2012-05-07-01,
- change default condition of insecure communication services to disabled,
- improve 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 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.

g. Latest news on ROS device security issue, http://www.ruggedcom.com/productbulletin/ros-security-page/, Web site last accessed May 25, 2012.

h.Siemens ProductCERT advisories, http://www.siemens.com/cert/advisories/, Web site last accessed May 25, 2012.

- 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

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.

i. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed May 25, 2012.