ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ALERT

ICS-ALERT-12-116-01A—RUGGEDCOM WEAK CRYPTOGRAPHY FOR PASSWORD VULNERABILITY

UPDATE A

April 27, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of a default backdoor user account with a password with trivial encoding. Proof-of-concept (PoC) exploit code affects RuggedCom RuggedSwitch and RuggedServer devices using Rugged Operating System (ROS). These network devices are used in a variety of network applications, including industrial control systems (ICSs).

According to this report, the vulnerability is exploitable by generating a password from known data about the device. This report was discovered and released by independent security researcher Justin W. Clarke following an attempted but unsuccessful coordination with the vendor.

ICS-CERT is issuing this alert to provide notice of the public report and identify baseline mitigations for reducing risks to this cybersecurity risk.

The report included vulnerability details and PoC exploit code for the following vulnerability:

Vulnerability Type	Exploitability	Impact
Weak cryptography for passwords[a]	Can be exploited remotely	Complete administrative control of the device

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

CVE-2012-1803[b] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned.

For details, please see US-CERT's vulnerability note: http://www.kb.cert.org/vuls/id/889195, website last accessed on April 25, 2012.

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,

[a] http://cwe.mitre.org/data/definitions/261.html, Website last access April 25, 2012.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1803, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

power plants, electrical substations, and military sites. Beyond simple 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.

The following ROS versions are known to be affected:

- 3.2.x and earlier (see note below)
- 3.3.x and above.

  Note: Customers who are running 3.2.x and earlier need to update to the latest release in order to have the capability to disable telnet and remote shell (rsh)

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

MITIGATION

RuggedCom is advising ROS customers to disable the rsh service and set the number of Telnet connections allowed to 0. The researcher has stated that the backdoor will not work over ssh (secure shell) or the web interface. With these recommendations, the backdoor will only be accessible via the local serial interface (RS232). ICS-CERT has not fully verified these mitigations.

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

ICS-CERT is coordinating with RuggedCom who has indicated that they intend to release a patch that removes the backdoor access to address this reported vulnerability. They plan to release this patch within the next month. In addition, RuggedCom has released a notification regarding this issue that can be accessed at http://www.ruggedcom.com/productbulletin/ros-security-page/.

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

ICS-CERT is currently coordinating with the security researcher, CERT/CC, and Siemens ProductCERT to identify useful mitigations. Siemens acquired RuggedCom earlier this year.

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. Control system devices should not directly face the Internet.[c]
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

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

[c] ICS-ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed April 25, 2012.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d]

Organizations that observe 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

ICS-CERT Operations Center
1-877-776-7585
ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats 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.

[d] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 25, 2012.