ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-354-01—RUGGEDCOM ROS HARD-CODED RSA SSL PRIVATE KEY

December 19, 2012

OVERVIEW

This advisory is a follow-up to the original alert titled ICS-ALERT-12-234-01A—KEY MANAGEMENT ERRORS IN RUGGEDCOM'S RUGGED OPERATING SYSTEM[a] that was published August 31, 2012, on the ICS-CERT Web page.

Independent researcher Justin W. Clarke of Cylance Inc., has identified the use of hard-coded RSA SSL private key in RuggedCom's Rugged Operating System (ROS). RuggedCom, an independent subsidiary of Siemens, has produced a new version of the ROS that mitigates this vulnerability.

This vulnerability could be exploited remotely. Exploits that target this vulnerability are publicly available.

AFFECTED PRODUCTS

The following RuggedCom products[b,c] are affected:

- Rugged OS, ver. 3.11 and prior
- ROX I OS firmware used by RX1000 and RX1100 series products. ROX I versions before and including ROX v1.14.5
- ROX II OS firmware used by RX5000 and RX1500 series products. ROX II versions before and including ROX v2.3.0

a. ICS-CERT Alert, https://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-234-01A.pdf. Web site last accessed December 18, 2012.

b. RuggedCom Website, http://www.ruggedcom.com/productbulletin/ros-security-page/. Web site last accessed December 18, 2012.

c. Siemens Security Advisory, https://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-622607.pdf. Web site last accessed December 18, 2012.

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy/

- RuggedMax Operating System Firmware used by the Win7000 and Win7200 base station units and the Win5100 and Win5200 subscriber (CPE) devices. All versions of the firmware released before and including 4.2.1.4621.22

IMPACT

The impact of exploiting this vulnerability will give an attacker the private SSL key for secure communications between client/user and a RuggedCom switch. The attacker can use the key to decrypt management traffic and create malicious communication to the RuggedCom network device.

This vulnerability has no impact on encrypted data traffic passing through RuggedCom ROS, ROX, or RuggedMax BS devices.

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, a Siemens Business, is a Canadian-based company with sales and distribution in over 25 countries around the world.

The affected product, Rugged Operating System (ROS) is the software operating system for RuggedSwitch and RuggedServer product families. ROS based devices are often deployed in critical infrastructure projects such as electrical substations, intelligent transportation systems, and rail wayside control.

RuggedCom/Siemens estimates that these products are used primarily in Canada, United States, Mexico, China, and Europe.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

KEY MANAGEMENT ERRORS[d]

Using publicly available software, the private SSL key can be extracted from the ROS binary file. This key can allow an attacker to establish a secure communication link with RuggedCom network devices and manipulate settings that would result in a denial of service condition.

d. CWE, http://cwe.mitre.org/data/definitions/320.html, CWE-320: Key Management Errors. Web site last accessed December 18, 2012.

CVE-2012-4698[e] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C). [f]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

DIFFICULTY

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

MITIGATION

ROS DEVICES

An update can be obtained from RuggedCom's Customer Support Team. Additional information is available on the RuggedCom homepage[g].

ROX DEVICES

ROX device customers are strongly encouraged to change their SSL and SSH keys. Application notes exist that explain how to change the SSL and SSH keys. Please consult App Note AN17 for ROX1.x versions of the firmware and App Note AN16 for ROX 2.x. These application notes can be obtained from RuggedCom's Customer Support Team.

e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4698. 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:M/Au:N/C:C/I:C/A:C). Web site last accessed December 18, 2012.

g RuggedCom Website, http://www.ruggedcom.com/productbulletin/ros-security-page/. Web site last accessed December 18, 2012.

RUGGEDMAX DEVICES

SSH SERVICE

For RuggedMax SSH service, the customer has the capability to generate new keys. Each device (subscriber or base station) can be triggered to generate a new SSH key by deleting the current key. Customers are strongly encouraged to generate new keys. A procedure on how to generate a new SSH key can be obtained from RuggedCom Customer Support Team.

HTTPS/SSL SERVICE

For the HTTPS access, a temporary solution exists with the current version of firmware to disable HTTPS access. For details on this procedure please contact the RuggedCom Customer Support Team.

Siemens recommendations the following mitigation strategies when deploying RuggedCom devices:

- Do not connect ROS, RuggedMax devices directly to an untrusted network such as the Internet.
- Establish a VPN solution to connect to an untrusted network such as the Internet.
- Check for any signs of unauthorized access to a device (e.g., by reviewing syslogs).
- Use industry best practices for security such as those defined by NERC-CIP.

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.

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.[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-12-146-01A—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 development of proper mitigations may put industrial control systems and the public at avoidable risk.

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html. Web site last accessed December 18, 2012.

i. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf. Web site last accessed December 18, 2012.