ICS-CERT ALERT

ICS-ALERT-12-234-01A—KEY MANAGEMENT ERRORS IN RUGGEDCOM'S RUGGED OPERATING SYSTEM

UPDATE A

August 31, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of a hard-coded RSA SSL private key within RuggedCom's Rugged Operating System (ROS). The vulnerability with proof-of-concept (PoC) exploit code was publicly presented by security researcher Justin W. Clarke of Cylance Inc. According to this report, the vulnerability can be used to decrypt SSL traffic between an end user and a RuggedCom network device.

ICS-CERT notified the affected vendor of the report and asked the vendor to confirm the vulnerability and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

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

Vulnerability Type	Remotely Exploitable	Impact
Key Management Errors[a]	Yes	Loss of System Integrity

--------- Begin Update A Part 1 of 3 --------

Further analysis by RuggedCom has identified similar vulnerabilities in the ROX (ROX I and ROX II) operating system firmware and the RuggedMax operating system firmware. A fix for the identified vulnerability in ROX is available. For the SSH service of RuggedMax, an interim mitigation for the identified vulnerability is also available.

a. MITRE, http://cwe.mitre.org/data/definitions/320.html, Web site last accessed August 31, 2012.

Siemens has reported the following are affected products:

- Devices using the ROS releases before and including ROS Main v3.11.0.
- ROX I OS firmware used by RX1000 and RX1100 series products. ROX I versions before and including ROX v1.14.5 are affected.
- ROX II OS firmware used by RX5000 and RX1500 series products. ROX II versions before and including ROX v2.3.0 are affected.
- 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.

--------- End Update A Part 1 of 3 ----------

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

Justin W. Clarke publicly reported that the RSA Private PKI key for SSL communication between a client/user and a RuggedCom switch can be identified in the ROS. An attacker may use the key to decrypt management traffic and create malicious communication to a RuggedCom network device.

--------- Begin Update A Part 2 of 3 --------

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

--------- End Update A Part 2 of 3 ----------

MITIGATION

ICS-CERT is currently coordinating with the vendor and security researcher to identify mitigations.

--------- Begin Update A Part 3 of 3 --------

Siemens has produced the following interim mitigations in Security Advisory SSA-622607:

ROS Devices

RuggedCom is currently working to prepare a firmware update addressing the identified vulnerability in the ROS-based devices.

Until a fix for the related vulnerability is released, RuggedCom recommends that owners/operators take precautions to prevent attackers from intercepting traffic between administration systems and ROS devices. Customers may also contact RuggedCom's Customer Support Team for assistance.

ROX Devices

ROX device customers are strongly encouraged to change their SSL and SSH keys. RuggedCom 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.

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.

RuggedCom's Customer Support Web site: http://www.ruggedcom.com/services/technical/.

Siemens ProductCERT has also issued Security Advisory SSA-622607 to address these vulnerabilities:

http://www.siemens.com/cert/advisories/

--------- End Update A Part 3 of 3 ----------

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should perform the following.

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[b]
- 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.

b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed August 31, 2012.

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

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

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
Email: ics-cert@dhs.gov

For CSSP 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 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.

c. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed August 31, 2012.