

Industry Advisory

ES-ISAC: RuggedCom Public Disclosure Allowing Remote Unauthorized Access

Initial Distribution: May 07, 2012

On April 24, 2012 a previously unknown backdoor for various RuggedCom communication devices was publicly posted. This backdoor provides administrative ("factory") access to the device.

[Why am I receiving this? >>](#)

[About NERC Alerts >>](#)

Status:

No Reporting is Required – For Information Only



PUBLIC: No Restrictions

[More on handling >>](#)

Instructions:

NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. **No particular response is necessary.** This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved reliability standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a reliability standard.

Distribution:

Initial Distribution: Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Owner, Transmission Operator.

[Who else will get this alert? >>](#)

[What are my responsibilities? >>](#)

Primary Interest Groups:

Cyber Security – Control Systems, Cyber Security – Corporate IT, Generation Engineering, Generation Operations, Physical Security, System Operations – Transmission Engineering, System Operators, System Operators – System Protection, Transmission Planning

Advisory: RuggedCom supplies hardened communications equipment such as serial device servers and Ethernet switches designed for industrial environments. It's "ROS®" operating system was found to contain a previously undocumented "factory" administrative account. This "factory" account used a hard-coded password which is based off of the device's Ethernet Media Access Control (MAC) Address. Once this easily discoverable MAC address is known, an attacker can use a simple publicly available script to generate the "factory" password and gain administrative access to the unit.

Device model numbers which are confirmed to contain this backdoor:

Layer 2 switches & servers	Small Layer 2 switches
RSG2100, RSG2100P, RSG2200, RSG2288, RSG2300, RSG2300P, RS969, RS416, RS416P, M2100, M2200, M969, RS8000, RS8000T, RS8000H, RS8000A, RS1600, RS1600T, RS1600F, RS400, RS401, RMC30	RS900, RS900L, RS900W, RS910, RS910L, RS910W, RS920L, RS920W, RS930L, RS930W, RS900M, RS900G, RS900GP, RS940G, i800, i801, i802, I803, RP110

* Please note that RuggedRouter (RX1000, RX1100) and RuggedBackBone (RX15xx, RX5000) products are not affected by this vulnerability as all their passwords are user controlled, including root.

The backdoor exists in ROS 3.3.x or greater for local serial console, telnet and rsh services, however prior versions (3.2.x or earlier) also include the same backdoor for https and ssh.

RuggedCom has committed to release new versions of ROS firmware that removes the undocumented factory account in the coming weeks. Recognizing their customers often standardize on a specific version of ROS, they will release updates for ROS v3.7, 3.8, 3.9, and 3.10. RuggedCom recommends that customers using ROS versions older than v3.7 upgrade to a newer version; however if this is not possible, RuggedCom will address software updates to older versions of the software on a case by case basis. Contact RuggedCom Support for more information.

Field devices with improper isolation or publicly accessible via the Internet face increased exposure. This increased exposure is due to a growing set of malicious actors—mostly amateurs or individuals lacking prior ICS knowledge—who are now equipped with free tools, such as Shodan and Metasploit, to identify and exploit these devices and systems. Through a combination of the above tools and Internet

facing industrial control systems, it is possible that hackers or hacktivist groups may cause sporadic component failures as they identify and interact with these devices. Additionally, other more knowledgeable adversaries would build their own attack tools based on these disclosures; such tools would be designed to cause a higher impact. Finally, malicious insiders may cause sporadic and hard-to-identify failures with direct local network access to the vulnerable RuggedCom devices.

Hardware Review Advice

- Prior to patching, review logs to confirm no unauthorized administrative access has been attained since the backdoor algorithm has been made publically available,
- If log files indicate unexplained access, confirm current passwords have not been changed and review configurations.
- Review recent substation break-ins; confirm the control house has not been accessed; if accessed confirm hardware has not been tampered with.

Mitigation Approaches

- Consider disabling the affected services with the below settings:
 - Administration – IP Services – Telnet Sessions Allowed: 0
 - Administration – IP Services – RSH Server: Disabled
 - Administration – Configure System Identification – Login Banner: Custom
- Consult your vendor regarding patching and mitigation options.
 - RuggedCom may be reached via 1-866-922-7975 or support@ruggedcom.com
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
 - If public network exposure is necessary, review contingency plans regarding tampering, such as unexpected reboots, loss of configuration, modification of configuration, and possible media exposure by hacktivist groups.
 - Allow only inbound addresses required for operation, block all other connections.
 - Filter outbound traffic allowing only connections required for operation.
- 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 a Virtual Private Network (VPN), and diligently monitor any allowed remote connections. Locate and change default user names and passwords; remove unnecessary accounts and change passwords for remaining accounts.

Background: The Shodan search engine continues to deliver accurate search results that identify Internet hosts to particular vendors and model numbers such as RuggedCom or other industrial control systems.

The increase of both local and global hacktivist groups supplies a potential threat agent with the intent, skills, and understanding to leverage Shodan, Metasploit, and other tools against various industrial control systems. The combination of fragile systems that may be Internet-facing and threat actors who now have the tools to identify and attack these systems has increased the risk to industrial control systems.

For further information on proper device isolation and remote access, please refer to the NERC Remote Access Guideline Alert (A-2011-08-24-01).

There are many other industrial control system devices that are also likely to have default or well-known passwords other than RuggedCom. It remains a best practice to change any default passwords, when possible, on all industrial control system devices and to isolate any device that may have a hard-coded factory default password.

Threat actors may impact operations in various ways once unauthorized factory access is gained. This impact may range from disrupting IT services such as SNMP alarms to active reconnaissance of network topology, to resetting the firmware and disrupting communications between devices. Such disruption may result in the loss of visibility of SCADA or remote control of field equipment.

Attachments

- ICS-ALERT-12-116-01A
- NERC ALERT A-2011-08-24-1 - REMOTE ACCESS GUIDANCE
- NERC GUIDANCE FOR SECURE INTERACTIVE REMOTE ACCESS
- RuggedCom Bulletin dated April 26 and 27, 2012

The ES-ISAC would like to acknowledge Justin W. Clarke, RuggedCom, Siemens, ICS-CERT and FERC for their contributions in the disclosure process.

Contact: Tim Roxey
Chief Cyber Security Officer
Director, ES-ISAC
North American Electric Reliability Corporation
1325 G Street NW, Suite 600
Washington, DC 20005
Tim.roxey@nerc.net
(202) 400-3013

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
(609) 452-1422
esisac@nerc.com

Alert ID: A-2012-05-07-01

You have received this message because you are listed as a primary compliance contact for your organization on the North American Electric Reliability Corporation's compliance registry. If you believe that you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact Trion King at NERC by calling (404) 446-9654 or emailing Trion directly at: trion.king@nerc.net.

North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560 www.nerc.com