SSA-472334: NTP Vulnerabilities in RUGGEDCOM ROX-based Devices

Publication Date	2015-12-18
Last Update	2015-12-18
Current Version	V1.0
CVSS Overall Score	3.9

SUMMARY

Siemens has released an update for ROX II-based devices and recommends mitigations for ROX I.

ROX-based devices from Siemens may be configured to use the NTP daemon from ntp.org for time synchronisation. The NTP daemon might be affected by recently discovered vulnerabilities.

AFFECTED PRODUCTS

- ROX II: All versions < 2.9.0
- ROX I: All versions

DESCRIPTION

ROX-based VPN endpoints and firewall devices are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 2 (http://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2015-7871)

An attacker could potentially make the NTP daemon accept time updates from non-specified NTP servers by sending specially crafted UDP packets to the NTP service (port 123/udp).

CVSS Base Score	5.0
CVSS Temporal Score	3.9
CVSS Overall Score	3.9 (AV:N/AC:L/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2015-7855)

An attacker could potentially crash the NTP daemon by sending specially crafted UDP packets to the NTP service (port 123/udp).

CVSS Base Score	1.7
CVSS Temporal Score	1.3
CVSS Overall Score	1.3 (AV:N/AC:H/Au:M/C:N/I:N/A:P/E:POC/RL:OF/RC:C)

Vulnerability 3 (CVE-2015-7704)

An attacker could potentially prevent the device from fetching time updates from its configured time servers by sending specially crafted UDP packets to the NTP service (port 123/udp) while the NTP daemon is running.

CVSS Base Score	5.0
CVSS Temporal Score	3.9
CVSS Overall Score	3.9 (AV:N/AC:L/Au:N/C:N/I:N/A:P/E:POC/RL:OF/RC:C)

Vulnerability 4 (CVE-2015-5300)

An attacker could potentially modify the time on the device by sending specially crafted UDP packets to the NTP service (port 123/udp) under certain circumstances.

CVSS Base Score	4.3
CVSS Temporal Score	3.4
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Mitigating Factors

The NTP service is deactivated on ROX I and ROX II-based devices by default.

If NTP is activated by the user, the configuration on ROX II (starting from version 2.6.0) and ROX I (all versions) by default contain the 'restrict default noquery' configuration which mitigates vulnerability 2. Any additional restrict commands for non-local addresses should also have the 'noquery' flag set.

Vulnerability 1: ROX I is not affected.

Vulnerability 3 and 4: Only the NTP client is affected.

SOLUTION

Siemens provides firmware update V2.9.0 for ROX II-based devices [1] which fixes the vulnerabilities.

For ROX I based devices and ROX II versions before ROX 2.9.0, Siemens recommends to implement the following mitigations:

- Block NTP packets from unknown peers using firewall rules
- Employ NTP time synchronization in trusted network only
- Ensure that the NTP configuration file contains the 'noquery' flag for all non-local restrict statements or deactivate NTP service if the functionality is not required.
- Configure NTP authentication and configure the 'notrust' flag for all non-local restrict statements on the NTP configuration (only applies to ROX II).

As a general security measure Siemens strongly advises to follow security recommendations in the product manual [2]. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] The firmware updates for the affected products can be obtained for free from the following contact points:
  - o Submit a support request online: http://www.siemens.com/automation/support-request
  - o Call a local hotline center: http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx

[2] Security recommendations for ROX-based devices are located in the manual: https://support.industry.siemens.com/cs/ww/en/ps/15320/man

[3] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.siemens.com/cert/operational-guidelines-industrial-security

[4] Information about Industrial Security by Siemens: https://www.siemens.com/industrialsecurity

[5] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2015-12-18): Publication Date

DISCLAIMER

See: https://www.siemens.com/terms_of_use