SSA-671683: NTP Vulnerabilities in Ruggedcom ROX-based Devices

Publication Date	2015-01-19
Last Update	2015-03-05
Current Version	V1.1
CVSS Overall Score	7.4

Summary:

ROX-based devices from Siemens use the NTP daemon from ntp.org for time synchronisation. These products might be affected by recent vulnerabilities in the NTP daemon.

Siemens has released an update for the affected products and recommends specific countermeasures until the fixes can be applied.

AFFECTED PRODUCTS

The following products could be affected by the NTP vulnerabilities in the default configuration:

- ROX 2: All versions < ROX 2.6.2

The following products are not exploitable in the default configuration, but a vulnerable NTP daemon is used and users may configure the system in a way so that it may be exploitable:

- ROX 1: All versions

DESCRIPTION

ROX-based VPN endpoints and firewalls 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 CVSSv2 scoring system (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-2014-9293)

If no “auth” key is set in the configuration file, the NTP daemon generates a weak random key on the fly for authentication.

CVSS Base Score	4.3
CVSS Temporal Score	3.2
CVSS Overall Score	3.2 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C)

Vulnerability 2 (CVE-2014-9294)

The NTP key generator used a weak seed to prepare a weak random number generator whose output was used to generate encryption keys.

CVSS Base Score	5.0
CVSS Temporal Score	3.7
CVSS Overall Score	3.7 (AV:N/AC:L/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C)

Vulnerability 3 (CVE-2014-9295)

Multiple vulnerabilities can be exploited if a user does not specify the command "restrict ... noquery" in the configuration file of the NTP daemon.

CVSS Base Score	10.0
CVSS Temporal Score	7.4
CVSS Overall Score	7.4 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)

Mitigating factors

All versions of ROX 1 are not affected to the vulnerabilities in the default configuration of NTP. If the NTP configuration was changed to a vulnerable configuration, please follow the steps in the section "Solution" to ensure that your device is not affected.

SOLUTION

Siemens has released an update for ROX 2 which fixes the vulnerabilities [1].

Until the update can be deployed, Siemens advises to apply the following steps to mitigate the risk:

- Either restrict access to the NTP service to trusted devices by setting the 'noquery' flag using the WebUI or CLI
- Or deactivate NTP service if the functionality is not required.

ROX 1 is not affected in the standard configuration. If alternative configurations are used, Siemens advises to apply the following steps:

- Either make sure that the following line is contained in your NTP configuration file:
  `restrict -4 default nomodify nopeer noquery notrap`
- Or deactivate NTP service if the functionality is not required.

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: http://support.automation.siemens.com/WW/view/en/79993488/133300

[3] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

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

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

HISTORY DATA

V1.0 (2015-01-19): Publication Date

V1.1 (2015-03-05): ROX 2 update released; Adjusted CVSS Scores to official fix

DISCLAIMER