SSA-860967: GNU Bash Vulnerabilities in Industrial Products

Publication Date 2014-10-06
Last Update 2015-02-13
Current Version V1.4
CVSS Overall Score 8.7

Summary:

Recent vulnerabilities in the Unix shell GNU Bash ("Shellshock") [1] affect several Siemens industrial products.

Siemens has released updates for all affected products.

AFFECTED PRODUCTS

The following products are affected by the GNU Bash vulnerabilities without major configuration modifications in the system's shell:

- ROX 1: All versions <= V1.16.0
  - Affected by vulnerability description 4
  - If DHCP client is activated: also affected by vulnerability description 1
- ROX 2: All versions < V2.6.0
  - Only if DHCP client is activated
  - Affected by vulnerability description 1
- APE Linux with ELAN installed (all versions)
  - Affected by vulnerability description 2

The following products are not exploitable by default, but a vulnerable version of GNU Bash is installed and users may configure the system in a way so that it may be exploitable (see also vulnerability description 3):

- APE Linux V1.0
- APE Linux V2: All versions <= V2.0.2
- SINUMERIK 808D, 828D, 840D sl: V4.4 - V4.5 SP3 (inclusive)
- SINUMERIK Operate Programming Package: All versions <= V4.6
- SINUMERIK Integrate CreateMyHMI / 3GL V4.5 SP3

DESCRIPTION

The recent GNU Bash vulnerabilities (CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278) [1] could allow attackers to perform remote code execution or privilege escalation on the affected devices. As product-specific exploits for the vulnerabilities are highly dependent on the system's configuration, specific exploit vector descriptions are 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 Description 1 (DHCP client attack vector)

The DHCP client is used for automatic IP address assignment of the device. Due to the GNU Bash vulnerabilities, malicious input sent to the client may lead to remote code execution.

CVSS Base Score	7.9
CVSS Temporal Score	6.5
CVSS Overall Score	6.5 (AV:A/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

Vulnerability Description 2 (APE ELAN attack vector)

The web interface of ELAN could allow unauthenticated users to perform privilege escalation due to the GNU Bash vulnerabilities.

CVSS Base Score	10.0
CVSS Temporal Score	7.8
CVSS Overall Score	7.8 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C)

Vulnerability Description 3 (Generic attack vector)

On the affected systems, GNU Bash is installed in a vulnerable version. However, this vulnerability cannot be exploited in the default configuration without major custom modifications by the user (such as installation of additional software or custom scripts).

No CVSS score has been calculated as the criticality of the vulnerability depends on the specific user modifications.

Vulnerability Description 4 (ROX1 Webmin attack vector)

The Webmin interface on ROX 1 could allow unauthenticated remote code execution, if an attacker has network access to the device. Siemens is aware of Internet-wide scans for Webmin installations.

CVSS Base Score	10.0
CVSS Temporal Score	8.7
CVSS Overall Score	8.7 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)

Mitigating Factor for Vulnerability Description 1:

The DHCP client must be activated.

Mitigating Factor for Vulnerability Description 4:

The Webmin interface must be reachable by the attacker.

SOLUTION

Siemens has provided updates for the following products and encourages customers to upgrade the products to this new version:

- ROX 1: Update to version 1.16.1 [2]
- ROX 2: Update to version 2.6.0 [2]
- SINUMERIK 808D, 828D, 840D: Update to version 4.5 SP4 [3]
- SINUMERIK Operate Programming Package: Upgrade to SINUMERIK Integrate CreateMyHMI / 3GL
- SINUMERIK Integrate CreateMyHMI / 3GL: Update to version 4.7 SP1 [3]
- APE 1.0 and APE 2.x: Update to newest version of bash [4]

Siemens also recommends protecting network access to all products except for perimeter devices such as ROX-based products with appropriate mechanisms. It is advised to follow recommended security practices [7] and to configure the environment according to operational guidelines [5] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] More information about the recent GNU Bash vulnerabilities can be found on the NVD vulnerability summary pages:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6277
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6278

[2] The firmware updates for the Ruggedcom ROX-based devices can be obtained for free from the following contact points:

- Submit a support request online:
  http://www.siemens.com/automation/support-request
- Call a local hotline center:
  http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx

[3] The update can be obtained from your local Siemens account manager.

[4] Instructions for upgrading APE can be found here:
http://support.automation.siemens.com/WW/view/en/104019656

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

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

[7] Recommended security practices by ICS-CERT:
http://ics-cert.us-cert.gov/content/recommended-practices

[8] 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 (2014-10-06):	Publication Date
V1.1 (2014-10-13):	Added fix for ROX 2 and adjusted CVSS score
V1.2 (2014-10-16):	Added Webmin vulnerability for ROX 1, added fix for ROX 1
V1.3 (2014-11-12):	Added updates for SINUMERIK and APE
V1.4 (2015-02-13):	Updated affected APE versions and solutions

DISCLAIMER