Security Advisory

Vulnerabilities in RUGGEDCOM ROX I Siemens RX1000

Author: Maxim Rupp
March, 2017

Direct references to file or code weaknesses that are mentioned in this advisory will not be disclosed to the public from my side due to ethical reasons. This advisory will be published after patches are available and in agreement with the vendor.

Index

Summary

Overview

According to Siemens Security Advisory SSA-327980, "RUGGEDCOM ROX I-based devices are affected by several vulnerabilities which could potentially allow attackers to perform actions with administrative privileges" (SUMMARY section, para. 1).

The following security issues refer to the standard web-based configuration interface of the Siemens RX1000 device.
The vulnerabilities have been discovered on a Siemens RX1000 device running firmware version ROX1.16.1; Webmin 1.160-2.rr880.

There are currently no known public exploits specifically targeting these vulnerabilities.

Affected Product

RUGGEDCOM ROX I: All versions

Impact

An authenticated, malicious remote user with low skills would be able to compromise the availability, integrity, and confidentiality of the Siemens RX1000 industrial device. The router effectively becomes an entry point into the network where it is located.

Successful exploitation of these vulnerabilities could significantly lower the security of the network area where the affected device is located. Impact to individual organizations depends on many factors that are unique to each organization.

Background

According to Siemens Security Advisory SSA-327980, "RUGGEDCOM 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" (DESCRIPTION section, para. 1).

Identified Security Issues

The following sections list information about the security issues. Please note that findings are not listed by their severity or impact. In addition to this, these findings may also be chained to increase the overall impact.

Improper Neutralization of Input During Web Page Generation (CVE-2017-2687)

According to Siemens Security Advisory SSA-327980, "The integrated web server at port 10000/TCP is prone to reflected Cross-Site Scripting attacks if an unsuspecting user is induced to click on a malicious link " (Vulnerability 2 section, para. 1). A CVSS v3 base score of 6.1 has been assigned.

The tested application processes malicious input with almost every available parameter. The application either fails to neutralize or incorrectly validates special characters such as "<", ">", "'", and "'".

These special characters will be interpreted as web-scripting elements that are processed by the browser. This leads to a possible implementation of Cross-Site Scripting attack (XSS). The XSS attack allows malicious user to execute arbitrary JavaScript code in a benign user's browsing context and thereby get access to sensitive data.

During the code review process about 20 potential vulnerable parameters have been discovered. All of them may lead to various types of XSS attack.

Path Traversal (CVE-2017-2686**)**

According to Siemens Security Advisory SSA-327980, "An authenticated user could read arbitrary files through the web interface at port 10000/TCP and access sensitive information" (Vulnerability 1 section, para. 1). A CVSS v3 base score of 6.5 has been assigned.

It was found that a lack of validation of user-supplied input in some functions of the web configuration interface leads to a Path Traversal vulnerability. The Path Traversal attack technique allows a malicious user to access files that reside outside the web document root directory on the host system.

This vulnerability allows a malicious user to steal sensitive information from the target host which could be used to mount further attacks against the host. For example, to obtain the password hashes of the local users or configuration files, which ultimately leads to disclosure of sensitive information to a third-party.

Access to the affected file was available for users with limited access rights.

Privilege Escalation (CVE-2017-2689**)**

According to Siemens Security Advisory SSA-327980, "An authenticated user could bypass access restrictions in the web interface at port 10000/TCP to obtain privileged file system access or change configuration settings" (Vulnerability 4 section, para. 1). A CVSS v3 base score of 8.8 has been assigned.

Improper Access Control

Based on the existing access control list (ACL), users with limited access rights from the "guest" group are denied access to many important functions from a security perspective in the device.

Some of these functions are:

```
download and upload files;
functions which are associated with backup, rollback or comparison of the existing archives;
configuration of the various modules
```

However, a malicious user could still get (partial or full) access to these functions, which violates the promises of the ACL.

For example, a malicious user was able to obtain access to highly sensitive files caused by the combination of the mentioned server misconfiguration and by accessing specific URLs on the web server.

By that, a malicious user could influence the correct functioning of some application components. This security issue allows to obtain sensitive information on the server-side that may aid in further attacks.

Unrestricted Upload of File with Dangerous Type

It was discovered that the application is completely missing verification of uploaded content. Moreover, the application functionality was absent of additional restrictions for accessing uploaded user data, which makes the application vulnerable to an arbitrary file upload attack.

This allows an attacker to drop scripts in the Webroot in order to execute arbitrary commands on the target host. Specifying the directory to upload was not strictly determined by the application but produced on client-side, which allows to control endpoints for file upload functionality.

This issue is found in the affected scenario of the application which was available to users with limited access rights. As a consequence, an attacker is able to use this weakness to gain access to other internal hosts.

Server Misconfiguration

The server was found to be affected by several common misconfiguration issues.

The first misconfiguration issue affects web server. It was found that the web server does not protect directory contents; the listing offers information that is not intended for public viewing.

This allows an attacker to get information about directory contents, which ultimately leads to information disclosure. In this particular case, these are highly sensitive backup files which contain configuration files from the application (including hashes of user passwords and other sensitive information).

The second misconfiguration of the server was that all running processes on the host are executed from a privileged "root" account.

Using this weakness a malicious user gains significant access to further compromise the infrastructure. The ability to sniff or modify network traffic allows for multiple attacks, such as DoS, MitM, or session hijacking. This could put other devices that are located in the same network as a RX1000 device under threat.

Cross-Site Request Forgery (CVE-2017-2688**)**

According to Siemens Security Advisory SSA-327980, "The integrated web server at port 10000/TCP could allow remote attackers to perform actions with the privileges of an authenticated user, provided the targeted user has an active session and is induced into clicking on a malicious link or into visiting a malicious website" (Vulnerability 3 section, para. 1). A CVSS v3 base score of 7.6 has been assigned.

The application protection against CSRF was based only on a weak verification of the "Referer" header. This is considered a systematic issue for the entire application.
The application does not sufficiently effective verify if a request was intentionally provided by the user who submitted the request. This means that unauthorized third-party websites which a user visits while she is logged in are able to trigger arbitrary requests on behalf of the user of the application.

Thus, it is possible that a malicious user can use a CSRF attack to modify the device configuration.

By utilizing the previously mentioned server misconfiguration and being able to specify the PRE-login banner of the SSH service a malicious user without ever having access to the Web interface is able to get contents of files from the host.

The following example combining the misconfiguration of the application and a CSRF attack illustrates the problem:

```
ssh <target host>
root:$1$defd1125$.7oSTu2I70AbeyzI5i3mQ0:17079:0:99999:7:::
daemon:*:16344:0:99999:7:::
```

```
bin:*:16344:0:99999:7:::
sys:*:16344:0:99999:7:::
[SKIP]
rupp@<target host>'s password:
```

Mitigation and Solution

For more detailed mitigation instructions, please see Siemens Security Advisory SSA-327980 at the following location: SSA-327980: Vulnerabilities in RUGGEDCOM ROX I

References

https://ics-cert.us-cert.gov/advisories/ICSA-17-087-01 — Siemens RUGGEDCOM ROX I
SSA-327980: Vulnerabilities in RUGGEDCOM ROX I

CVE-2017-2686 (CWE-285: Improper Authorization)
CVE-2017-2687 (CWE-79: Improper Neutralization of Input During Web Page Generation)
CVE-2017-2688 (CWE-352: Cross-Site Request Forgery)
CVE-2017-2689 (CWE-285: Improper Authorization)

I would like to thank Siemens ProductCERT team for the collaboration.