SSA-631949: Ripple20 and Intel SPS Vulnerabilities in SPPA-T3000 Solutions

Publication Date: 2020-07-14
Last Update: 2022-02-17
Current Version: V1.1
CVSS v3.1 Base Score: 10.0

SUMMARY

SPPA-T3000 solutions from Siemens Energy are affected by vulnerabilities that were disclosed by

- JSOF research lab (“Ripple20”, https://www.jsof-tech.com/ripple20/) for the TCP/IP stack used in APC UPS systems
- Intel for the Server Platform Services (SPS, https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html) used in SPPA-T3000 Application Server and Terminal Server hardware.

The advisory provides information to what amount SPPA-T3000 solutions are affected. Detailed information, including solution and mitigation measures, are available for SPPA-T3000 customers in the Siemens Energy Customer Portal (https://cep.siemens-energy.com/).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SPPA-T3000 APC UPS with NMC card AP9630 or AP9631: All versions only affected by CVE-2020-11896	APS UPS systems are affected by multiple Ripple20 vulnerabilities, including CVE-2020-11896 and 14 more. The T3000 specific CVSS Environmental Score is 3.6 (Severity: low). Please contact your Siemens Energy service management organisation how to mitigate the Ripple20 vulnerabilities in T3000 solutions. See further recommendations from section Workarounds and Mitigations
SPPA-T3000 Application Server: All versions only affected by CVE-2020-0545	When running on a HP ProLiant DL360 Gen10 server, the SPPA-T3000 Application Server is affected in the Intel Server Platform Services (SPS) included in the server hardware. The T3000 specific CVSS Environmental Score is 3.6 (Severity: low). Please contact your Siemens Energy service management organisation how to obtain the patch for the Intel SPS system of the server hardware. See further recommendations from section Workarounds and Mitigations

SPPA-T3000 Terminal Server: All versions only affected by CVE-2020-0545	When running on a HP ProLiant DL360 Gen10 server, the SPPA-T3000 Terminal Server is affected in the Intel Server Platform Services (SPS) included in the server hardware. The T3000 specific CVSS Environmental Score is 3.6 (Severity: low). Please contact your Siemens Energy service management organisation how to obtain the patch for the Intel SPS system of the server hardware. See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Implement mitigations described in the SPPA-T3000 security manual
- Restrict access to the Application Highway using the SPPA-T3000 Firewall
- External components should be connected only to the SPPA-T3000 DMZ; no bridging of an external network to either the Application- or Automation highways is allowed
- Perform regular updates of the SPPA-T3000 (e.g. by using the Security Server if available)
- Implement mitigations provided in the customer information letter distributed via the customer service portal
- Please contact your local Siemens Energy representative if you need help at securing your SPPA-T3000 installation

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens Energy strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens Energy strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens Energy strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

SPPA-T3000 is a distributed control system mostly used in fossil and large scale renewable power plants.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2020-0545

An integer overflow in Intel Server Platform Services (SPS) may allow a privileged user to potentially enable denial of service via local access.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2020-11896

The Treck TCP/IP stack on affected devices improperly handles length parameter inconsistencies. Unauthenticated remote attackers may be able to send specially crafted IP packets which could lead to a denial of service condition or remote code execution.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-130: Improper Handling of Length Parameter Inconsistency

ADDITIONAL INFORMATION

For more details regarding the vulnerabilities refer to

- Siemens Energy Customer Portal: https://cep.siemens-energy.com/
- JSOF Ripple20 Vulnerabilities: https://www.jsof-tech.com/ripple20/
- Schneider Electric Security Notification SEVD-2020-174-01: https://www.se.com/ww/en/download/document/SEVD-2020-174-01/
- Intel Security Advisory INTEL-SA-00295: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html
- HP Enterprise Security Bulletin HPESBHF03999: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf03999en_us

The CVSS Environmental Scores for SPPA-T3000 solutions from Siemens Energy are based on the Base and Temporal Scores and were determined as follows:

- CVE-2020-11896: Environmental Score 3.6 (Low)

  CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C/AR:H/MAV:A/MAC:H/MS:U/MC:N/MI:N/MA:L
- CVE-2020-0545: Environmental Score 3.6 (Low)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C/MAC:H

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2020-07-14): Publication Date
V1.1 (2022-02-17): Editorial changes, assigned to Siemens Energy

TERMS OF USE