SSA-211752: Multiple NTP-Client Related Vulnerabilities in SIMATIC CP 443-1 OPC UA

Publication Date: 2021-06-08
Last Update: 2022-02-08
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

All versions of the SIMATIC CP 443-1 OPC UA contain multiple vulnerabilities in the underlying third party component NTP.

Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0): All versions	Currently no remediation is planned See 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:

- Deactivate NTP-based time synchronization of the device, if enabled. The feature is disabled by default
- Configure an additional firewall to prevent communication to port udp/123 of an affected device

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SIMATIC CP 343-1 and CP 443-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300/S7-400 CPUs.

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-2015-7705

The rate limiting feature in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to have unspecified impact via a large number of crafted requests.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2015-7853

The datalen parameter in the refclock driver in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a negative input value.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Vulnerability CVE-2015-8138

NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to bypass the origin timestamp validation via a packet with an origin timestamp set to zero.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-1547

An off-path attacker can cause a preemptible client association to be demobilized in NTP 4.2.8p4 and earlier and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92 by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-1548

An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. After making this switch, the client in NTP 4.2.8p4 and earlier and NTPSec aa48d001683e5b791a743ec9c575aaf7d867a2b0c will reject all future legitimate server responses. It is possible to force the victim client to move time after the mode has been changed. ntpq gives no indication that the mode has been switched.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L/E:U/RL:O/RC:C
CWE	CWE-19: Data Processing Errors

Vulnerability CVE-2016-1550

An exploitable vulnerability exists in the message authentication functionality of libntp in ntp 4.2.8p4 and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92. An attacker can send a series of crafted messages to attempt to recover the message digest key.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-2518

The MATCH_ASSOC function in NTP before version 4.2.8p9 and 4.3.x before 4.3.92 allows remote attackers to cause an out-of-bounds reference via an addpeer request with a large hmode value.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2016-4953

ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (ephemeral-association demobilization) by sending a spoofed crypto-NAK packet with incorrect authentication data at a certain time.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2016-4954

The process_packet function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (peer-variable modification) by sending spoofed packets from many source IP addresses in a certain scenario, as demonstrated by triggering an incorrect leap indication.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’)

Vulnerability CVE-2016-4955

ntpd in NTP 4.x before 4.2.8p8, when autokey is enabled, allows remote attackers to cause a denial of service (peer-variable clearing and association outage) by sending (1) a spoofed crypto-NAK packet or (2) a packet with an incorrect MAC value at a certain time.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2016-4956

ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (interleaved-mode transition and time change) via a spoofed broadcast packet. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-1548.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-7431

NTP before 4.2.8p9 allows remote attackers to bypass the origin timestamp protection mechanism via an origin timestamp of zero. NOTE: this vulnerability exists because of a CVE-2015-8138 regression.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-7433

NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-682: Incorrect Calculation

Vulnerability CVE-2016-9042

An exploitable denial of service vulnerability exists in the origin timestamp check functionality of ntpd 4.2.8p9. A specially crafted unauthenticated network packet can be used to reset the expected origin timestamp for target peers. Legitimate replies from targeted peers will fail the origin timestamp check (TEST2) causing the reply to be dropped and creating a denial of service condition.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2017-6458

Multiple buffer overflows in the ctl_put* functions in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allow remote authenticated users to have unspecified impact via a long variable.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

ADDITIONAL INFORMATION

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 (2021-06-08): Publication Date
V1.1 (2022-02-08): No remediation planned for SIMATIC CP 443-1 OPC UA

TERMS OF USE