Cyber Security Advisory #05/2021

Multiple Vulnerabilities in Automation Runtime NTP Service

Document Version: 1.0

First published: 2021-05-27
Last updated: N/A (Initial version)

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

B&R provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall B&R or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if B&R or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from B&R, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Executive Summary

Automation Runtime (AR) features an NTP service based on ntpd, a reference implementation of the Network Time Protocol (NTP).
Affected AR versions include an outdated version of ntpd which is affected by a large number of vulnerabilities as detailed in Appendix A: List of ntpd vulnerabilities.

Affected Products

Affected products: Automation Runtime (AR)
Affected versions: 4.8 and below

The following versions are **not affected:**

- AR 4.9 and above

Corrective Actions or Resolution

Upgrade your AR-powered B&R products to AR version 4.9 or above.

The NTP service included in Automation Runtime 4.9 and above includes a current, supported version of ntpd. At the time of writing version 1.0 of this advisory, the version of ntpd in AR 4.9 is the most current version available.

Workarounds and Mitigations

In case you cannot upgrade your systems to AR 4.9 or above, you can choose from the following options to reduce risks associated with the NTP service:

1. If your AR systems do not need to provide time information to other systems, disable the NTP server on those systems.
   Please note that the NTP server is disabled by default in Automation Runtime.

2. If you do not need to synchronize your AR systems with NTP servers, disable the NTP client on those systems.
   Please note that the NTP client is disabled by default in Automation Runtime.

3. In case you must use the NTP server on an AR system, choose from the following options to reduce NTP-based risks:
   a. Allow NTP traffic to/from trusted NTP clients[1] only
   b. Monitor the network for malicious NTP traffic going to/coming from the AR system
   c. Filter malicious NTP traffic going to/coming from the AR system
   d. Monitor NTP server operations on your AR systems (server availability, correctness of advertised time, NTP-related log entries, etc.)
   e. Use suitable measures listed in our “General recommendations for safeguarding control systems[2]”

[1] “Trusted NTP clients” refers to systems you can rely on security-wise. An example of a trusted NTP client would be an internal system configured and operated by your organization according to security best practices. An untrusted NTP client would be a system out in the Internet using the AR system as an NTP server.

[2] See section “Supporting information and guidelines”

4. In case you must use the NTP client on an AR system, choose from the following options to reduce NTP-based risks:
    a. Use trusted NTP servers[3] only
    b. Allow NTP traffic to/from trusted NTP servers only
    c. Monitor the network for malicious NTP traffic targeting the AR system
    d. Filter malicious NTP traffic targeting the AR system
    e. Monitor NTP client operations on your AR systems (correctness of system time, NTP-related log entries, etc.)
    f. Use suitable measures listed in our “General recommendations for safeguarding control systems”

Supporting information and guidelines

The B&R Cyber Security webpage provides further information including Cyber Security guidelines like the “General recommendations for safeguarding control systems”. Please find these resources here: https://www.br-automation.com/en/service/cyber-security/

Document History

Version	Date	Description
1.0	2021-05-27	Initial version

[3] “Trusted NTP servers” refers to NTP servers you can rely on security-wise. An example of a trusted NTP server would be an internal NTP server configured and operated by your organization according to security best practices. An example of an untrusted NTP server would be an NTP pool member server – if you synchronize for example to 0.pool.ntp.org, you do not even know which server you are talking to.

Appendix A: List of ntpd vulnerabilities

CVE ID	CVSS-Score	Description
CVE-2009-3563	6.4	ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by using MODE_PRIVATE to send a spoofed (1) request or (2) response packet that triggers a continuous exchange of MODE_PRIVATE error responses between two NTP daemons.
CVE-2013-5211	5.0	The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests, as exploited in the wild in December 2013.
CVE-2014-9293	7.5	The config_auth function in ntpd in NTP before 4.2.7p11, when an auth key is not configured, improperly generates a key, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.
CVE-2014-9294	7.5	util/ntp-keygen.c in ntp-keygen in NTP before 4.2.7p230 uses a weak RNG seed, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.
CVE-2014-9295	7.5	Multiple stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to execute arbitrary code via a crafted packet, related to (1) the crypto_recv function when the Autokey Authentication feature is used, (2) the ctl_putdata function, and (3) the configure function.
CVE-2014-9296	5.0	The receive function in ntp_proto.c in ntpd in NTP before 4.2.8 continues to execute after detecting a certain authentication error, which might allow remote attackers to trigger an unintended association change via crafted packets.
CVE-2014-9750	5.8	ntp_crypto.c in ntpd in NTP 4.x before 4.2.8p1, when Autokey Authentication is enabled, allows remote attackers to obtain sensitive information from process memory or cause a denial of service (daemon crash) via a packet containing an extension field with an invalid value for the length of its value field.
CVE-2015-5300	5.0	The panic_gate check in NTP before 4.2.8p5 is only re-enabled after the first change to the system clock that was greater than 128 milliseconds by default, which allows remote attackers to set NTP to an arbitrary time when started with the -g option, or to alter the time by up to 900 seconds otherwise by responding to an unspecified number of requests from trusted sources, and leveraging a resulting denial of service (abort and restart).
CVE-2015-7691	5.0	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted packets containing particular autokey operations. NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7692	5.0	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7701	5.0	Memory leak in the CRYPTO_ASSOC function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (memory consumption).
CVE-2015-7702	4.0	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7703	4.3	The "pidfile" or "driftfile" directives in NTP ntpd 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77, when ntpd is configured to allow remote configuration, allows remote attackers with an IP address that is allowed to send configuration requests, and with knowledge of the remote configuration password to write to arbitrary files via the :config command.
CVE-2015-7704	5.0	The ntpd client in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service via a number of crafted "KOD" messages.

CVE-2015-7705	7.5	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.
CVE-2015-7849	6.5	Use-after-free vulnerability in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to possibly execute arbitrary code or cause a denial of service (crash) via crafted packets.
CVE-2015-7850	4.0	ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to cause a denial of service (infinite loop or crash) by pointing the key file at the log file.
CVE-2015-7851	3.5	Directory traversal vulnerability in the save_config function in ntpd in ntp_control.c in NTP before 4.2.8p4, when used on systems that do not use '\' or '/' characters for directory separation such as OpenVMS, allows remote authenticated users to overwrite arbitrary files.
CVE-2015-7852	4.3	ntpq in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted mode 6 response packets.
CVE-2015-7853	7.5	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.
CVE-2015-7854	6.5	Buffer overflow in the password management functionality in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted key file.
CVE-2015-7855	4.0	The decodenetnum function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (assertion failure) via a 6 or mode 7 packet containing a long data value.
CVE-2015-7871	7.5	Crypto-NAK packets in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to bypass authentication.
CVE-2015-7973	5.8	NTP before 4.2.8p6 and 4.3.x before 4.3.90, when configured in broadcast mode, allows man-in-the-middle attackers to conduct replay attacks by sniffing the network.
CVE-2015-7974	4.0	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key."
CVE-2015-7975	2.1	The nextvar function in NTP before 4.2.8p6 and 4.3.x before 4.3.90 does not properly validate the length of its input, which allows an attacker to cause a denial of service (application crash).
CVE-2015-7976	4.0	The ntpq saveconfig command in NTP 4.1.2, 4.2.x before 4.2.8p6, 4.3, 4.3.25, 4.3.70, and 4.3.77 does not properly filter special characters, which allows attackers to cause unspecified impact via a crafted filename.
CVE-2015-7977	4.3	ntpd in NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (NULL pointer dereference) via a ntpdc reslist command.
CVE-2015-7978	5.0	NTP before 4.2.8p6 and 4.3.0 before 4.3.90 allows a remote attackers to cause a denial of service (stack exhaustion) via an ntpdc relist command, which triggers recursive traversal of the restriction list.
CVE-2015-7979	5.0	NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (client-server association tear down) by sending broadcast packets with invalid authentication to a broadcast client.
CVE-2015-8138	5.0	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.
CVE-2015-8139	5.0	ntpq in NTP before 4.2.8p7 allows remote attackers to obtain origin timestamps and then impersonate peers via unspecified vectors.
CVE-2015-8140	5.8	The ntpq protocol in NTP before 4.2.8p7 allows remote attackers to conduct replay attacks by sniffing the network.
CVE-2015-8158	4.3	The getresponse function in ntpq in NTP versions before 4.2.8p9 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (infinite loop) via crafted packets with incorrect values.

CVE-2016-1547	5.0	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.
CVE-2016-1548	6.4	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.
CVE-2016-1549	4.0	A malicious authenticated peer can create arbitrarily-many ephemeral associations in order to win the clock selection algorithm in ntpd in NTP 4.2.8p4 and earlier and NTPsec 3e160db8dc248a0bcb053b56a80167dc742d2b74 and a5fb34b9cc89b92a8fef2f459004865c93bb7f92 and modify a victim's clock.
CVE-2016-1550	5.0	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.
CVE-2016-1551	2.6	ntpd in NTP 4.2.8p3 and NTPsec a5fb34b9cc89b92a8fef2f459004865c93bb7f92 relies on the underlying operating system to protect it from requests that impersonate reference clocks. Because reference clocks are treated like other peers and stored in the same structure, any packet with a source ip address of a reference clock (127.127.1.1 for example) that reaches the receive() function will match that reference clock's peer record and will be treated as a trusted peer. Any system that lacks the typical martian packet filtering which would block these packets is in danger of having its time controlled by an attacker.
CVE-2016-2516	7.1	NTP before 4.2.8p7 and 4.3.x before 4.3.92, when mode7 is enabled, allows remote attackers to cause a denial of service (ntpd abort) by using the same IP address multiple times in an unconfig directive.
CVE-2016-2517	4.9	NTP before 4.2.8p7 and 4.3.x before 4.3.92 allows remote attackers to cause a denial of service (prevent subsequent authentication) by leveraging knowledge of the controlkey or requestkey and sending a crafted packet to ntpd, which changes the value of trustedkey, controlkey, or requestkey. NOTE: this vulnerability exists because of a CVE-2016-2516 regression.
CVE-2016-2518	5.0	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.
CVE-2016-2519	4.9	ntpd in NTP before 4.2.8p7 and 4.3.x before 4.3.92 allows remote attackers to cause a denial of service (ntpd abort) by a large request data value, which triggers the ctl_getitem function to return a NULL value.
CVE-2016-4953	5.0	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.
CVE-2016-4954	5.0	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.
CVE-2016-4955	4.3	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.
CVE-2016-4956	5.0	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.

CVE-2016-4957	5.0	ntpd in NTP before 4.2.8p8 allows remote attackers to cause a denial of service (daemon crash) via a crypto-NAK packet. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-1547.
CVE-2016-7426	4.3	NTP before 4.2.8p9 rate limits responses received from the configured sources when rate limiting for all associations is enabled, which allows remote attackers to cause a denial of service (prevent responses from the sources) by sending responses with a spoofed source address.
CVE-2016-7427	3.3	The broadcast mode replay prevention functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via a crafted broadcast mode packet.
CVE-2016-7428	3.3	ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via the poll interval in a broadcast packet.
CVE-2016-7429	4.3	NTP before 4.2.8p9 changes the peer structure to the interface it receives the response from a source, which allows remote attackers to cause a denial of service (prevent communication with a source) by sending a response for a source to an interface the source does not use.
CVE-2016-7431	5.0	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.
CVE-2016-7433	5.0	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."
CVE-2016-7434	4.3	The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a crafted mrulist query.
CVE-2016-9310	6.4	The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.
CVE-2016-9311	7.1	ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet.
CVE-2017-6451	4.6	The mx4200_send function in the legacy MX4200 refclock in NTP before 4.2.8p10 and 4.3.x before 4.3.94 does not properly handle the return value of the snprintf function, which allows local users to execute arbitrary code via unspecified vectors, which trigger an out-of-bounds memory write.
CVE-2017-6458	6.5	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.
CVE-2017-6460	6.5	Stack-based buffer overflow in the reslist function in ntpq in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote servers have unspecified impact via a long flagstr variable in a restriction list response.
CVE-2017-6462	4.6	Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.
CVE-2017-6463	4.0	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote authenticated users to cause a denial of service (daemon crash) via an invalid setting in a :config directive, related to the unpeer option.
CVE-2017-6464	4.0	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote attackers to cause a denial of service (ntpd crash) via a malformed mode configuration directive.
CVE-2018-12327	7.5	Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11 allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source.
CVE-2018-7182	5.0	The ctl_getitem method in ntpd in ntp-4.2.8p6 before 4.2.8p11 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mode 6 packet with a ntpd instance from 4.2.8p6 through 4.2.8p10.

CVE-2018-7183	7.5	Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array.
CVE-2018-7184	5.0	ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2015-7704.
CVE-2018-7185	5.0	The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association.
CVE-2018-8956	5.0	ntpd in ntp 4.2.8p10, 4.2.8p11, 4.2.8p12 and 4.2.8p13 allow remote attackers to prevent a broadcast client from synchronizing its clock with a broadcast NTP server via soofed mode 3 and mode 5 packets. The attacker must either be a part of the same broadcast network or control a slave in that broadcast network that can capture certain required packets on the attacker's behalf and send them to the attacker.
CVE-2019-8936	5.0	NTP through 4.2.8p12 has a NULL Pointer Dereference.
CVE-2020-11868	5.0	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.
CVE-2020-13817	5.8	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.
CVE-2020-15025	4.0	ntpd in ntp 4.2.8 before 4.2.8p15 and 4.3.x before 4.3.101 allows remote attackers to cause a denial of service (memory consumption) by sending packets, because memory is not freed in situations where a CMAC key is used and associated with a CMAC algorithm in the ntp.keys file.