ntpsec SOS Fund Audit Fix Log

This document lists all of the issues found by the Cure53 audit of the NTPsec version of NTP, and the steps taken to fix them. The fixes were made by Eric S. Raymond and Gary E. Miller of the NTPsec team. All fixes were verified against the respective references in the document and re-verified against the latest available revision from the repository, which was a8be9781 at the time. Any commentary is from the NTPsec team except where noted. They are presented in the same order as the audit report.

Identified Vulnerabilities

NTP-01-012 NTPsec: Authenticated DoS via Malicious Config Option (High)

Fixed in commit d837e2fd:
https://gitlab.com/NTPsec/ntpsec/commit/d837e2fd8259f120a5e716508a8ce1999c9e83ee

Nikolai Krein (Cure53): *Looks ok. Manually verified.*

VERIFIED

NTP-01-015 NTPsec: Regression in ctl_putdata() leads to Endless Loop (High)

Fixed in commit f75f890d:
https://gitlab.com/NTPsec/ntpsec/commit/f75f890ddbd7fa677fe8e34fa5319fd07941f00d

Nikolai Krein (Cure53): *The patch pretty much got reverted again. Fine.*

VERIFIED

NTP-01-016 NTPsec: Denial of Service via Malformed Config (High)

Fixed in d06bf4e4:
https://gitlab.com/NTPsec/ntpsec/commit/d06bf4e4b2d388708f4c5c15ff09094573c16b7c

Note: this prevention predated ntpsec’s receipt of the report.

Nikolai Krein (Cure53): *Seems to do it. Manually verified.*

VERIFIED

Miscellaneous Issues

NTP-01-001 NTPsec: Makefile does not enforce Security Flags (Low)

Partial work in commits 1414f7a1, 12ce52e1, b3054a61, a500711e, b5d0ce3f, 9e27a194, 9bdb59ca, 15a12e8c, c799b77f, 80bacbbc, e0db0107, 391c17ea, 807358f9, 10ae96dd, 16fd97c6a, 74f7ec81, 6ac1f01c5, 6a255733, 2ea68bb5, 10782450, 31ea8cfc, 9803c39e, c3c9e6e2, b339e2dc, ba046444, 8bf1f929, 4ab962f3, 1e6ecdee, 400e38a8, 51544a0a, and 0c2352a4.

Final fix in commit 8ee10dec:
https://gitlab.com/NTPsec/ntpsec/commit/8ee10deccc2a6ffd1bff614d4f19bac1cc79168c

Added waf rules to check for available security options and use the best ones available.

Nikolai Krein (Cure53): *This looks ok, despite apparently omitting FORTIFY_SOURCE. But given the difficulties with that option, I'm fine with that.*

```
(gdb) checksec
CANARY    : ENABLED
FORTIFY   : disabled
NX        : ENABLED
PIE       : ENABLED
RELRO     : FULL
(gdb) quit
```

VERIFIED

NTP-01-003 NTPsec: Improper use of snprintf() in mx4200_send() (Low)

Fixed in commits aa1084bc, 93acee72 and c88b93e7:
https://gitlab.com/NTPsec/ntpsec/commit/c88b93e7a4d4dd2c9f1c0fe990e7dff27f772e95

VERIFIED

NTP-01-004 NTPsec: Potential Overflows in ctl_put() functions (Medium)

Fixed in commit f75f890d:
https://gitlab.com/NTPsec/ntpsec/commit/f75f890ddbd7fa677fe8e34fa5319fd07941f00d

Followup in ffc76878:
https://gitlab.com/NTPsec/ntpsec/commit/ffc76878ecbf8fa60b8a225ad4e96bcd582c72be

VERIFIED

NTP-01-005 NTPsec: Off-by-one in Oncore GPS Receiver (Low)

Fixed in d59b89ff:
https://gitlab.com/NTPsec/ntpsec/commit/d59b89ffc240f348f29b535854bf2f2df8cab065

VERIFIED

NTP-01-013 NTPsec: Inclusion of obsolete NTPclassic-dependent Script (Info)

ntpsec: This is not a real issue; the script does useful work in the NTPsec distribution. attic/ntpver queries the running ntpd daemon for its version and prints it out. Like this:

```
spidey attic # ./ntpver
ntpsec-0.9.6+4127
```

The script is simple, just a handy tool:

```
spidey attic # cat ntpver
#!/bin/sh
# print version string of NTP daemon
# Copyright (c) 1997 by Ulrich Windl
# Modified 970318: Harlan Stenn: rewritten...
# usage: ntpver hostname

ntpq -c "rv 0 daemon_version" $* | awk '/daemon_version/ { print
2 }'
```

Pretty harmless.

VERIFIED