ntp SOS Fund Audit Fix Log

The master list of checkins is here:
http://bk.ntp.org/ntp-stable/?DATE=20170211..20170309&PAGE=changes

VERIFIED

Identified Vulnerabilities

NTP-01-002 NTP: Buffer Overflow in ntpq when fetching reslist (Medium)

Fix: http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=589f58574daOkdmCkyXNpBeidQfotw

Fixed by limiting the length of *val* via *strlen(val))* < *sizeof(row.flagstr)*.

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

Fix: http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58a03410Wgv3k8FUIty8KGhffw-O4Q

Fixed by changing the parsing in *create_unpeer_node*, instead of patching *config_unpeers*.

VERIFIED

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

Fix: http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58a02199vI1qv8JAaprTc-gvvJ05Fg

Fixed by introducing an additional sanitization check for *T_Ttl* and *T_Mode* when calling *create_peer_node*.

VERIFIED

Miscellaneous Issues

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

Fix:
http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58b01858BDuBSxU40fKTiW1WT1M8AQ

Fixed by providing a way in the build system to trigger OS-specific hardening flags.

VERIFIED

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

Fix:
http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=589f6a59geVwfxo2jMu6V8GxzwUENQ

Return value of vsnprintf is checked correctly now.

VERIFIED

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

Fix: http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58a008c2PtxGYR8g6fLpoaFecrZ-zQ

Much cleaner solution using snprintf and correct return value checks has been introduced.

VERIFIED

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

Fix: http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58a0982b4Us3fEKsxxwdgL43NfkIDw

Length check has been replaced.

VERIFIED

NTP-01-006 NTP: Copious amounts of Unused Code (Info)

The NTP team disputes, in various cases, either that the code is unused or that removing it will result in a net benefit when maintainability is taken into account.

NOT VERIFIED

NTP-01-007 NTP: Data Structure terminated insufficiently (Low)

Fix:
http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58a08ecfhwReHRRwhO9LAupytFPOfg

VERIFIED

NTP-01-008 NTP: Stack Buffer Overflow from Command Line (Low)

Fix:
http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58a08ecfhwReHRRwhO9LAupytFPOfg

strcat is replaced with *snprintf*, including correct return value check.

VERIFIED

NTP-01-009 NTP: Privileged execution of User Library code (Low)

Fix:
http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58bc191bDZd_XnGYlOxrP6OMXLbkOw

Note that the NTP team assessed the severity of this issue as Medium rather than the Low that the Cure53 team assigned it.

The registry code was refactored and overrides %PPSAPI_DLLS%. As a fallback getenv() is still supported for compatibility, but will be phased out with the next major release.

VERIFIED

NTP-01-010 NTP: ereallocarray()/eallocarray() underused (Info)

Fix:
http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58b89dd858FkqPk48ACoSQvi8Rv7Tw

Also, when calling *oreallocarray,* made sure that memory is zero initialized.

VERIFIED

NTP-01-011 NTP: ntpq_stripquotes() returns incorrect Value (Info)

Fix:
http://bk1.ntp.org/ntp-stable/?PAGE=patch&REV=58a04868cNA4vy24WAI8cH1sK8y9og

strlen is removed and replaced with the delta from start to end.

VERIFIED

NTP-01-014 NTP: Buffer Overflow in DPTS Clock (Low)

Fix: http://bk1.ntp.org/ntp-stable/?PAGE=cset&REV=58a0592bal7oYBqUMCqId4WgiuiOqw

Additional check inside the for loop limits the incoming data.

VERIFIED