chrony SOS Fund Audit Fix Log

Identified Vulnerabilities

CHR-01-001 chronyc: Null Pointer Deref in manual list Response Handler (Low)

Fix: https://git.tuxfamily.org/chrony/chrony.git/commit/?id=f40b0024bd43b24d4d3a97ba28def9b4fdfc336e

Miroslav Lichvar (chrony): This fixes the UTI_TimeToLogForm() function to check for gmtime() errors. This could have caused a crash due to dereferencing a NULL pointer in chronyc when printing a crafted response to the "manual list" request.

VERIFIED

CHR-01-002 General: Wrappers around malloc() do not check for Overflows (Low)

Fix: https://git.tuxfamily.org/chrony/chrony.git/commit/?id=7ffee735247353c6af7871d41dd064ffb80b064a

Miroslav Lichvar (chrony): While I agree this should definitely be fixed, it doesn't look like a security issue to me, at least with the current code which is using the macros. In the example that was given in the report, I don't think ARR_GetSize() would return a size that could overflow, because it was already checked in an assert() when the records array was allocated. In any case, I think all arrays that can grow with NTP/cmdmon requests either have a hardcoded maximum size (records in clientlog.c), or are much smaller than memory allocated for structures to which they are related to (sources, sort_list, sel_sources in sources.c grow with number of NCR and SST instances), so their size couldn't overflow before a memory allocation failed.

Mike Wege (Cure53): *Agreed. We classified the Issue as a Miscellaneous Low because simply we couldn’t find an exploitable scenario for it. It is just a precaution to avoid possible future problems.*

VERIFIED