Network Device Interpretation # 202026

Clarification of audit date information

Status: ☒ *Active* □ *Inactive*

Date: *18-Jan-2021*

End of proposed Transition Period (to be updated after TR2TD process): *18-Feb-2021*

Type of Change: □ Immediate application ☒ Minor change □ Major change

Type of Document: ☒ *Technical Decision* □ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPPv2.2e*

Affected Section(s): *FAU_GEN.1.2*

Superseded Interpretation(s): *None*

Issue:

The term 'date' in FAU_GEN.1.2 is unclear. There seems to be no information that clarifies the requirements on the date in audit records. It is unclear whether the year needs to be included in the audit record or not, or if the month and day are sufficient.
The vendor currently implements the syslog protocol and produces syslog audit records without the year in the date. A redacted example record is provided below:
May 4 16:15:39.812 <DEVICE> login.audit: INFO Too many failed login attempts on <USER>, user account is locked.
On the TOE, the individual audit records are written to files that are stored within the /var/log/ directory. These files are named with the year, month, day, and hour, and contain the individual audit records from that hour, separated by line breaks (e.g. the filename syslog-2020101411 contains all entries from October 14, 2020 on 11th hour. Each line within the file is a single audit record that contains the detailed timestamp as shown above).

<u>Resolution:</u>
The CCTL requests clarification on what details are expected to be included in the 'date' field of individual audit records. As well as if it is acceptable for this information to be included as metadata (e.g. filename). It is our opinion that the approach of this product is effectively the same as including the year within the record, and the vendor does not believe this approach will have any negative impact on traditional audit log analysis.

Resolution:

To address the issue described above, the following paragraphs shall be added to Application Note 3 for FAU_GEN.1.2:

<new>

The date and time information for any audit event shall be recorded as part of each audit record to ensure the timing of the event can be unambiguously determined from the data contained in the audit record. The representation of date and time information recorded for each event needs to allow unanimous determination of at least day, month and year information for the date and hours, minutes and second information for the time.

</new>

Rationale:

FAU_GEN.1.2a.) clearly requires that date and time of the event needs to be recorded with each audit record. As the purpose of the date and time information is to unambiguously allow the administrator to determine when each recorded event happened, the date information needs to include the information about the year.

As encoding parts of the date and time information (e.g. year) in some sort of meta data (e.g. filename) would require mechanisms (either at local storage, remote storage or both) to determine the full date and time information which are not covered by the current version of NDcPP, encoding parts of the date and time information in meta data is not in agreement with the current version of NDcPP.

Further Action:

None

Action by Network iTC:

None