



NiCE

NetApp Manageability SDK 9.8P10における脆弱性CVE-2026-49844

https://kb-ja.netapp.com/on-prem/ontap/da/Host-Utilities/Host-Utilities-KBs/Vulnerability_CVE-2026-498...

Updated: Fri, 23 Oct 2026 10:16:34 GMT

環境

- NetApp Manageability SDK (NMSDK)
- Apache Log4jバージョン2.13.1～2.25.4
- NMSDKを実行するLinux管理仮想マシン
- NMSDKを使用するONTAP自動化環境

問題

- NetApp Manageability SDK (NMSDK) 9.8P10を実行しているLinux管理VMで、脆弱性スキャンにより以下の検出結果が報告されました。
- スキャンにより、zexplore.jarおよびmanageontap-9.8P10.jar内にApache Log4jバージョン2.19.0が検出され、Apache Log4jの修正バージョン2.25.5が推奨されています。
- プラグイン出力：

Path: /data/netapp-manageability-sdk-9.8P10/zedi/zexplore.jar

Installed version: 2.19.0

Fixed version: 2.25.5

Path: /data/netapp-manageability-sdk-9.8P10/lib/java/classes/

manageontap-9.8P10.jar

Installed version: 2.19.0

Fixed version: 2.25.5

- 説明：

The version of Apache Log4j on the remote host is affected by a vulnerability (CVE-2026-49844): Improper encoding of non-finite floating-point values during MapMessage JSON serialization in Apache Log4j API produces output that is not valid JSON.

- 主な症状：

Vulnerability detected in NMSDK JAR files due to outdated Log4j.

Customer asks if upgrading NMSDK to 9.8P12 will resolve the issue.

Concern if affected JAR files will be updated automatically with SDK upgrade.

Requests for guidance on remediation or workarounds.