Security Advisory Report - OBSO-2003-01

Apache Log4j SocketServer Class Log Data Handling Insecure Deserialization Remote Code Execution (CVE-2019-17571)

Release Date: 2020-03-03 15:18:31
Last Update: 2020-03-13 13:28:05

Summary

Apache Log4j up to version 1.2.17 contains a flaw that is triggered as the SocketServer class accepts log data from untrusted network traffic, which it then insecurely deserializes. This may allow a remote attacker to potentially execute arbitrary code.

At present none of the evaluated Unify products are effected by the vulnerability.

Details

Unify is evaluating the impact of the vulnerability. First evaluation of products has shown that products may not be impacted as SocketServer class and the vulnerable methods are not used.

The Security Advisory will be updated as additional information is available.

Affected Products

Products not affected:

OpenScape 4000
OpenScape Business (Platform)
OpenScape Voice
OpenScape SBC
OpenScape Branch
OpenScape UC
OpenScape Contact Center

OpenScape Contact Center Extensions
OpenScape Concierge
OpenScape Xpressions
OpenScape Deployment Service
OpenScape Common Management Portal
OpenScape Media Server
OpenScape Fault Management
OpenScape Accounting Management
OpenScape Xpert
OpenScape Xpert System Manager
OpenStage/OpenScape Desk Phone IP SIP
OpenStage/OpenScape Desk Phone IP HFA
OpenScape Desk Phone CP SIP
OpenScape Desk Phone CP HFA
OpenScape Desktop Client Personal Edition
OpenScape UC Webclient
OpenScape Alarm Response
Circuit
OpenScape Fusion for IBM Notes
OpenScape Business Admin Portal
OpenStage Gateview Application

Recommended Actions

Frequently check for updates of this advisory on our website.
https://unify.com/en/support/security-advisories

References

- https://logging.apache.org/log4j/1.2/
- https://www.suse.com/support/update/announcement/2020/suse-su-20200054-1/
- https://www.suse.com/support/update/announcement/2020/suse-su-202014267-1/
- https://security-tracker.debian.org/tracker/CVE-2019-17571
- https://issues.apache.org/jira/browse/AMQ-7370

Advisory: OBSO-2003-01, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

© Unify Software and Solutions GmbH & Co. KG 2020
Otto-Hahn-Ring 6
D-81739 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.