

Security Advisory Report - OBSO-2003-02

GhostCat. Apache Tomcat Unspecified Local File Inclusion. (CVE-2020-1938)

Release Date: 2020-03-12 16:01:33

Last Update: 2020-03-27 18:57:53

Summary

Apache Tomcat **versions 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99**, contains a local file inclusion (LFI) flaw due to the program not properly sanitizing user input, specifically path traversal style attacks (e.g. '../..'). With a specially crafted request, a remote attacker can include arbitrary files from the targeted host. This may allow disclosing file contents or executing files like JSP scripts. Such attacks are limited due to the script only calling files already on the target host.

Exploit for CVE-2020-1938

Impact: Remote file read, potentially upload of files with malicious code

Description: Ability to read any file in a webapp

Impact: Disclosure of sensitive information

How: Using AJP connection, which is usually found on port 8009

Unify is evaluating the impact of the vulnerability.

Details

This vulnerability can allow an attacker to run existing code on a vulnerable webserver which uses AJP. Thus it is not considered critical since no new code is uploaded with this vulnerability.

A First evaluation of our products has shown that products may not be impacted as **Apache JServ Protocol (AJP)** is not used.

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

More information about CVE-2020-1938 can be found [on Mitre.org site](#)

Latest Update on 2020-03-27:

Products affected

OpenScape SESAP server (fix planned in V2.1.1.2 / expected on 2020-04-24)

Affected Products

Products not affected:

OpenScape 4000 Platform
OpenScape 4000 Manager (with Security Checklist applied)
OpenScape Business (Platform)
OpenScape Voice
OpenScape SBC
OpenScape Branch
OpenScape UC Application
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 Deployment Service
OpenScape Desk Phone CP SIP
OpenScape Desk Phone CP HFA
OpenScape Desktop Client Personal Edition
OpenScape UC Webclient
OpenScape Alarm Response
OpenScape Fusion for IBM Notes
Circuit
Openscape Media Server
OpenScape Business Admin Portal
OpenScape UC Facade server

Products affected

OpenScape SESAP server (fix planned in V2.1.1.2 / expected on 2020-04-24)

Recommended Actions

Make sure the Security Checklist for **OpenScape 4000 Manager** is applied and the firewall is active. For the **OpenScape SESAP Server** make sure that the Windows Firewall is active and port 8009 is closed.

Frequently check for updates of this advisory on our website.

<https://unify.com/en/support/security-advisories>

References

- <https://securityboulevard.com/2020/02/patch-your-tomcat-and-jboss-instances-to-protect-from-ghostcat-vulnerability-cve-2020-1938-and/>
- <https://www.bleepingcomputer.com/news/security/active-scans-for-apache-tomcat-ghostcat-vulnerability-detected-patch-now/>
- <https://www.zdnet.com/article/ghostcat-bug-impacts-all-apache-tomcat-versions-released-in-the-last-13-years/>
- <http://tomcat.apache.org/security-8.html>
- <http://tomcat.apache.org/security-7.html>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-1938>

Advisory: OBSO-2003-02, 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
obs@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.