Security Advisory Report - OBSO-2210-01

Apache Commons Text Insecure Interpolation Defaults Input Handling Arbitrary Code Execution (CVE-2022-42889)

Release Date:	2022-10-26 14:35:13
Last Update:	2022-11-08 11:48:45
Version:	1.1

Summary

A high severity vulnerability has been found in the Apache Commons Text library. The flaw exists in the StringSubstitutor.createInterpolator() class/method and can allow an attacker to execute arbitrary code if the vulnerable code can be triggered.

The library contains a standard lookup format for interpolation, but versions 1.5 through 1.9 were found to contain some other default lookups that could accept untrusted input from a remote attacker, leading to remote code execution.

Version 1.10.0 of Apache Commons Text disables these problematic formats by default, and users are advised to upgrade to this version immediately.

We are currently analyzing the impact of the Atos Unify portfolio. At the current state of the evaluation we have identified a few products that deploy a vulnerable version of Apache Commons Text. We currently are not aware of a possibility to exploit the vulnerability within Atos Unify products that have Apache Commons Text deployed.

The initial severity is rated medium.

Details

The flaw exists in the StringSubstitutor.createInterpolator() class/method and can allow an attacker to execute arbitrary scripts passed to the created interpolator object.
This can be used by passing a string “${prefix:name}” where the prefix is one of below mentioned lookup strings.

- “script” - execute a script on the target in the JVM
- “dns” - performing dns resolution
- “url” - makes a call to the entered URL including remote servers

The “script”, “dns”, or “url” lookups would allow a crafted string to execute arbitrary scripts when passed to the interpolator object. The attacker can send a crafted payload remotely using “script”, “dns” and “url” lookups to achieve arbitrary remote code execution.
Exploitation requirements:

In order to exploit the vulnerabilities, the following requirements must be met:

- The application has to accept user-controlled input that is subsequently processed by one of the following methods of the affected component: o StringLookupFactory.INSTANCE.interpolatorStringLookup().lookup() o StringSubstitutor.createInterpolator().replace()
- Nashorn engine is effectively not available in modern JDKs but JEXL which is also affected is.

Base on this the vulnerability is not necessarily trivial to exploit, and which greatly depends on the context of use of the Apache Commons Text library.

Affected Products

Products confirmed affected
An update will be provided when fix versions for the affected components are available or the component will be removed from the product.

Additional information is provided in a Knowledge Base Article KB000105043 in the Unify Support Portal.

Products delivering Apache Commons Text (severity rating medium)
OpenScape Contact Center V10 and V11
OpenScape UC V10

Products delivering Apache Commons Text (severity rating low)
OpenScape Fault Management V11 and V12 (fixes planned in V11R0.01.37 and V12R0.00.20)

Products confirmed not affected

Circuit
Unify Phone
Atos Unify OpenScape Business V3
Atos Unify OpenScape Voice (simplex deployments) V10
Atos Unify OpenScape 4000 V8 and V10 Platform
Atos Unify OpenScape 4000 V8 and V10 Assistant
Atos Unify OpenScape 4000 V8 and V10 CSTA
Atos Unify OpenScape 4000 V8 and V10 Loadware
Atos Unify OpenScape Voice (duplex deployments) V10
Atos Unify OpenScape Cordless IP V2
Atos Unify OpenScape First Response ESRP V9
Atos Unify OpenScape First Response BCF V10
Atos Unify OpenScape First Response ESAPP V1
Atos Unify OpenScape First Response PSS V1
Atos Unify OpenScape First Response MSBF V2
Atos Unify OpenScape First Response NGLS V1
Atos Unify OpenScape Alarm Response Professional V4 and V5
Atos Unify Virtual Care Collaboration Service V1
Atos Unify OpenScape Xpert Clients V7
Atos Unify OpenScape Xpert MLC V7
Atos Unify OpenScape Xpert System Manager V7
Atos Unify OpenScape Branch V10

Atos Unify OpenScape SBC V10
Atos Unify OpenScape Contact Media Service V10,V11
Atos Unify OpenScape Fusion for Office V2
Atos Unify OpenScape Extensions for MS Outlook V2
Atos Unify OpenScape Fusion for Notes V2
Atos Unify OpenScape Web Collaboration V7
Atos Unify OpenScape Concierge V4
Atos Unify OpenScape Xpressions V7
Atos Unify OpenScape Personal Edition V7
Atos Unify OpenScape Media Server V9
Atos Unify OpenScape 4000 Manager V8 and V10
Atos Unify OpenScape Common Management Platform V10
Atos Unify OpenScape Composer V2
Atos Unify OpenScape Deployment Service V10
Atos Unify OpenScape Accounting Management V4 and V5
Atos Unify OpenScape Voice Trace Manager V8
Atos Unify OpenScape Voice Survival Authority
Atos Unify OpenScape Desk Phones CP SIP
Atos Unify OpenScape Desk Phones CP HFA
Atos Unify OpenScape Desk Phones IP SIP V3
Atos Unify OpenScape Desk Phones IP HFA V3
Atos Unify OpenScape WLAN Phone WL3 and WL4
Atos Unify OpenScape DECT Phone S5 and SL5
Atos Unify OpenScape DECT Phone R6, S6 and SL6
Atos Unify OpenScape WLAN Phone Wireless Service Gateway
AC Win SL V3
HiPath CAP V3.0
HiPath DS-Win V4
Atos Unify OpenScape Backup & Recovery Services
Atos Unify OpenScape Sesap V2
Atos Unify OpenScape License Management CLA/CLM

Recommended Actions

Workarounds:

OpenScape Contact Center

- Refer to Knowledge Article KB000105043 in the Atos Unify Support portal

References

- https://blogs.apache.org/security/entry/cve-2022-42889
- https://www.tarlogic.com/blog/cve-2022-42889-critical-vulnerability-affects-apache-commons-text/
- https://www.contrastsecurity.com/security-influencers/cve-2022-42889-dont-panic-do-patch-contrast-security
- Researchers Keep a Wary Eye on Critical New Vulnerability in Apache Commons Text (darkreading.com)
- https://www.rapid7.com/blog/post/2022/10/17/cve-2022-42889-keep-calm-and-stop-saying-4shell/
- https://twitter.com/pwntester/status/1582321752566161409
- https://www.computerweekly.com/news/252526218/Apache-vulnerability-a-risk-but-not-as-widespread-as-Log4Shell
- https://www.darkreading.com/application-security/apache-commons-vulnerability-patch-but-dont-panic

Version Change History

Version	Date	Description
1.0	26.10.2022	- Initial release
1.1	08.11.2022	- Updates on the description - Updated the references - OpenScape Fault Management V11 and V12 (fixes planned in V11R0.01.37) and V12R0.00.20)

Advisory: OBSO-2210-01, status: ready for review
Security Advisories are released as part of Atos 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

Otto-Hahn-Ring 6
D-81739 München
www.unify.com