PUBLIC - FOR EXTERNAL USE: (TLP: WHITE)

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Security Advisory Report - OBSO-2310-02

Google WebP (libwebp) utils/huffman_utils.c BuildHuffmanTable() Function Stream Decoding Heap Buffer Overflow (CVE-2023-4863,CVE-2023-5129)

Status:	Update Release
Release Date:	2023-12-11 14:15:04
Last Update:	2023-12-13 12:39:12
Version:	1.1

Summary

Google WebP (libwebp) contains an overflow condition in the BuildHuffmanTable() function in utils/huffman_utils.c that is triggered when decoding streams containing an invalid Huffman tree. This may allow a context-dependent attacker to cause a heap-based buffer overflow, potentially allowing the execution of arbitrary code.

The severity rating is high to medium. The severity of the vulnerability depends on how the libwebp library is used in the product.

Details

The CVSS3.1 base score is 8.8 (high)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Affected components;

- libwebp versions 0.5.0 to 1.3.1
- Any software that utilizes the WebP codec through the libwebp library are impacted.
- A list of applications that uses the WebP codec are mentioned in here

Affected Products

Product statements are related only to supported product versions. Products which have reached End of Support (M44) status are not considered.

Products confirmed affected

Circuit (see Additional Notes 2)
Atos Unify OpenScape Business V3 (X1/X3/X5/X8) before V3R3.0.1_007 (available) (see Additional Notes 3)
Atos Unify OpenScape Business S before V3R3.0.1_007 (available) (see Additional Notes 3)
Atos Unify OpenScape Xpert Clients V7 (Linux) before V7.0.8.4 (available) and V7.5.2.0 (available)
Atos Unify OpenScape Xpert Clients V7 (Windows) (fix planned in V8 R0.20.0 for Q2/2024) (see Additional Notes 4)
Atos Unify OpenScape Contact Center V10 before V10R4.16.0 (available) (see Additional Notes 5)
Atos Unify OpenScape Contact Center V11 before V11 R1.12.0 (available) (see Additional Notes 5)
Atos Unify OpenScape Contact Media Service V11 before V11R1.5.0 (available)
Atos Unify OpenScape UC Application V10 (Windows) before V10 R5.7.0 (available) (see Additional Notes 6)
Atos Unify OpenScape UC Application V10 (macOS) (fix planned in V10 R5.8.0 for December 2023) (see Additional Notes 6)
Atos Unify OpenScape Voice (simplex deployments) V10 (refer to OpenScape UC Desktop Application)
Atos Unify Virtual Care Collaboration Service V1 (fix planned in V1R0.161.0)

Products confirmed not affected

Unify Phone
Atos Unify OpenScape 4000 V10 Platform
Atos Unify OpenScape 4000 V10 Assistant
Atos Unify OpenScape 4000 V10 CSTA
Atos Unify OpenScape 4000 V10 Loadware
Atos Unify OpenScape Voice (duplex deployments) V10
Atos Unify OpenScape Cordless IP V2
Atos Unify OpenScape Alarm Response Professional V4
Atos Unify OpenScape Alarm Response Professional V5
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 Fusion for Office V2
Atos Unify OpenScape Extensions for MS Outlook V2
Atos Unify OpenScape Fusion for Notes V2
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 V10
Atos Unify OpenScape Common Management Platform V10

Atos Unify OpenScape Composer V2
Atos Unify OpenScape Deployment Service V10
Atos Unify OpenScape Fault Management V11 and V12
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 V1
Atos Unify OpenScape Desk Phones CP SIP V2
Atos Unify OpenScape Desk Phones CP HFA V1
Atos Unify OpenScape Desk Phones CP HFA V2
Atos Unify OpenScape Desk Phones IP SIP V3
Atos Unify OpenScape Desk Phones IP HFA V3
Atos Unify OpenScape WLAN Phone WL4
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 License Management CLA
Atos Unify OpenScape License Management CLM
Atos Unify OpenScape Sesap V2
Atos Unify OpenScape Backup & Recovery Services

Additional Notes

1) Linux based applications running on Suse or Debian Linux

Apply the provided patches of the operating system suppliers in order to mitigate the exposure of the operating system.

2) Circuit

The exposure of the Circuit Desktop Application is considered low.
Circuit does not support WebP and WebM media and previews during the conversation screens thus it's impossible to trigger using a conversation message.
There is certain exposure when SSO login is configured for a Circuit tenant but the exposure of the vulnerability is considered low.

3) OpenScape Business

The myPortal@work application is impacted by the vulnerability but the impact of the vulnerability is reduced. As myPortal@work is not loading remote content a remote code execution is hence not deemed to be possible. A code change is planned to be implemented within V3 R3 FR1 that will entirely block the processing of Webp images.

For OpenScape Business S an update of the Suse operating system is recommended.

4) OpenScape Xpert

OpenScape Xpert Softclient (Windows):
The attack surface is reduced, as users can't visit any URL, they need to be preconfigured by an administrator in the Xpert System Manager.

5) OpenScape Contact Center

This vulnerability affects the Agent Portal Desktop Application.

6) OpenScape UC Application

Internal reference: UCBE-33535
The UC Desktop Application cannot be exploited remotely without authentication. The attack vector is reduced:
For OpenScape UC Desktop Application on a local user installation:
The CVSS3.1 base score is 7.0 (high)
CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
For the OpenScape UC Desktop Application on a All Users Installation
The CVSS3.1 base score is 6.4 (medium)
CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

Recommended Actions

Customers are advised to update the systems with the available fixes.
Update operating systems for Linux based applications.

References

https://nvd.nist.gov/vuln/detail/CVE-2023-4863
https://www.suse.com/security/cve/CVE-2023-4863.html
https://security-tracker.debian.org/tracker/CVE-2023-4863
WebP 0day - Google Assign New CVE for libwebp Vulnerability (cyberkendra.com)
The WebP 0day (isosceles.com)

Version Change History

Version	Date	Description
1.0	11.12.2023	- Initial release
1.1	13.12.2023	- Updated summary statement

Advisory: OBSO-2310-02, status: update release
Security Advisories are released as part of Mitel 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 2023
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.