an atos business

Security Bulletin

Heap buffer overflow in libwepp

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-488
Created	:	10 November 2023
Version	:	2.1
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	26 January 2024
Keywords	:	CVE-2023-4863

TLP:CLEAR

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

FOR PUBLIC USE

List of changes

Version	Date	Description
1.0	2023-11-10	First remediation version
2.1	2024-01-26	TLP-CLEAR version

Executive summary

The vulnerability CVE-2023-4863 was found in the open source Libwebp library and affects browsers such as Mozilla, Chrome and Edge.

On September 6th, 2023 Apple Security Engineering and Architecture (SEAR) and The Citizen Lab at the University of Toronto reported a critical vulnerability affecting an image compression library used in Chromium and other software solutions that support WebP images.

WebP is an image format that offers superior lossless and lossy compression for images on the Web. Thanks to WebP, developers and webmasters have the ability to generate more compact, high-quality images, which leads to a significant improvement in the loading speed of web pages.

Google developed an open source library for manipulating images in WebP format, known as Libwebp, providing tools and functionality for encoding and decoding images in this format.

The CVE-2023-4863 vulnerability can be found in this library, specifically in the BuildHuffmanTable function used to validate the input data. The problem lies in the fact that this function allocates extra memory if the existing table is not large enough for the input data, allowing arbitrary data to be written outside of the bounds set in memory, when processing a malicious WebP image, which can lead to arbitrary code execution.

This vulnerability not only affects the Mozilla Firefox browser or others based on Chromium (Google Chrome, Microsoft Edge, Opera, Vivaldi, Brave) but also affects applications such as Thunderbird, Honeyview, Signal Electron, Affinity, Gimp, Inkscape, LibreOffice, Telegram, ffmpeg or 1Password, among others.

The Chromium team has already reported the exploitation of this zero-day in the wild, so it is recommended to update affected products as soon as possible.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-4863	7.1	Out-of-bounds Write AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

In the context of HPC, the prerequisites for exploitability are different from the generic case.

Affected products

The following products depends on libwebp component which should be updated to remain secure

HPC Management Software	RHEL 7.9	RHEL 8.6 EUS	RHEL 8.7 (EOL)	RHEL 8.8
SMC xScale XRV	Not affected	Fixed by RHSA-2023:5189	Unpatched	Fixed by RHSA-2023:5309

Although Eviden makes effort to provide accurate and complete information, Eviden shall not be liable if the above table is incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

Recommendations

The main solution is to urgently update the affected products to the new released versions that correct this vulnerability. Migration to supported versions of RHEL is also recommended.

Available Vendor Patches

Erratas for Red Hat Enterprise Linux have been published:

- https://access.redhat.com/security/cve/CVE-2023-4863

Available Workarounds

No workaround is available.

Available Mitigations

Configurations which automatically apply security updates will fix the vulnerability transparently.

Available Exploits/PoC

The Chromium team has already reported the exploitation of this zero-day in the wild.

References

1. https://bugzilla.redhat.com/show_bug.cgi?id=2238431
2. https://access.redhat.com/security/cve/CVE-2023-4863

3. https://nvd.nist.gov/vuln/detail/CVE-2023-4863
4. https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
5. https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/
6. https://chromium.googlesource.com/webm/libwebp
7. https://stackdiary.com/critical-vulnerability-in-webp-codec-cve-2023-4863/

Glossary of terms

Term	Description
Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. https://www.first.org/tlp/
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update

About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden makes effort to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information provides is provided “as is” without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

https://support.bull.com/ols/product/security/psirt

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

[1] *Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2023.*