Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google Patches Critical Zero-Day Exploits Found at Pwn2Own

Date of Publication	Last updated date	Admiralty Code	TA Number
March 28, 2024	April 4, 2024	A1	TA2024122

Summary

First Seen: March 26, 2024
Affected Platform: Google Chrome
Impact: Google patched multiple zero-day vulnerabilities in Chrome (CVE-2024-2886, CVE-2024-2887 and CVE-2024-3159) from Pwn2Own Vancouver 2024, allowing arbitrary code execution. Updating Chrome is essential to ensure you're protected.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-2886	Google Chrome WebCodecs Use After Free Vulnerability	Google Chrome	✓	✗	✓
CVE-2024-2887	Google Chrome WebAssembly Type Confusion Vulnerability	Google Chrome	✓	✗	✓
CVE-2024-3159	Google Chrome V8 Out of Bounds Vulnerability	Google Chrome	✓	✗	✓

Vulnerability Details

#1

Google has addressed multiple vulnerabilities in Chrome, including three zero-day vulnerabilities disclosed during the Pwn2Own Vancouver 2024 hacking competition. The first zero-day, CVE-2024-2886, is a high-severity use-after-free flaw in WebCodecs. The second, CVE-2024-2887, is a high-severity type confusion issue in WebAssembly. Both vulnerabilities allowed remote attackers to execute arbitrary code via crafted HTML pages.

#2

The third, CVE-2024-3159, is a high-severity Out-of-bounds memory read issue in V8 JavaScript engine. This flaw allowed attackers to potentially steal sensitive information or crash browsers through crafted websites.

#3

Additionally, Google addressed CVE-2024-2883, CVE-2024-2885 and CVE-2024-3158, which are a critical severity use-after-free vulnerabilities, as well as CVE-2024-3156, an inappropriate implementation in V8. Google has updated the Stable channel to versions 123.0.6312.105/.106/.107 for Windows and Mac and 123.0.6312.105 for Linux, with updates rolling out gradually. Earlier in January, Google patched another zero-day (CVE-2024-0519) in Chrome's V8 JavaScript engine.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-2886	Google Chrome prior to 123.0.6312.86	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-2887	Google Chrome prior to 123.0.6312.86	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-843
CVE-2024-3159	Google Chrome prior to 123.0.6312.105	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-119

Recommendations

Apply Security Updates: Ensure that Chrome is updated to the latest version (123.0.6312.105/.106/.107 for Windows and Mac, and 123.0.6312.105 for Linux) to receive the fixes for these vulnerabilities. Regularly check for updates and apply them promptly.

Enable Automatic Updates: Configure Chrome to automatically install updates to ensure that security patches are applied as soon as they become available, reducing the window of exposure to potential threats.

Implement Web Filtering: Employ web filtering solutions or browser extensions that can help block access to potentially malicious websites known for distributing malware or exploiting vulnerabilities.

Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0001 Initial Access	T1203 Exploitation for Client Execution
T1588 Obtain Capabilities	T1588.005 Exploits	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application

Patch Details

Update Chrome browser to the latest version 123.0.6312.105/.106/.107 for Windows and Mac and 123.0.6312.105 for Linux.

Link:
https://www.google.com/intl/en/chrome/?standalone=1

References

https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html

https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html

https://twitter.com/thezdi/status/1770927914831274115

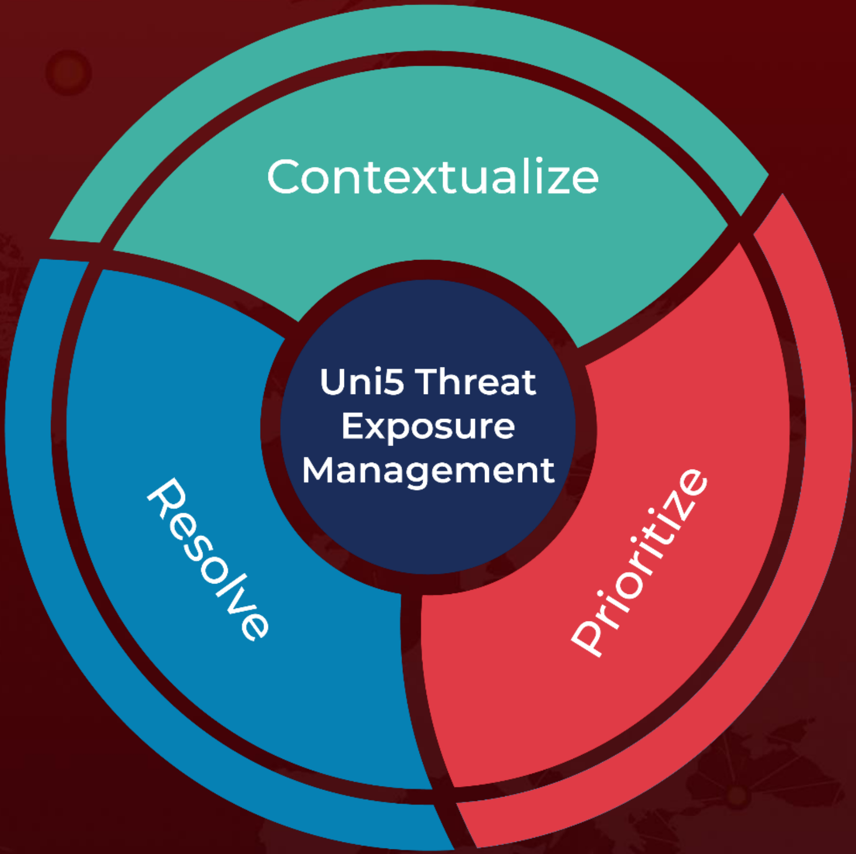
https://thecyberthrone.in/2024/03/28/google-addressed-zeroday-vulnerabilities-identified-in-pwn2own/

https://www.hivepro.com/threat-advisory/google-fixes-first-actively-exploited-chrome-zero-day-of-2024/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 28, 2024 • 3:30 AM

More at www.hivepro.com