FORTINET

OUTBREAK ALERTS

Google Chromium WebP Vulnerability

Critical open source library flaw actively exploited

https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
CVEs: CVE-2023-4863

The Google Chromium WebP heap buffer overflow vulnerability has been actively been exploited in the wild. The exploitation of the vulnerability is through a crafted image that can impact the affected applications to crash or lead to arbitrary code execution.

Background

Google developed an open source library Libwebp for manipulating images in WebP format. The libary provides tools for encoding and decoding images that leads to a significant improvement in loading of web pages. The Libwebp library is built-in on Google Chromium that is consumed by popular applications such as Google Chrome, Microsoft Edge, Microsoft Teams, Mozilla Firefox and Mozilla Thunderbird.

Announced

Sept 06, 2023: The Chromium WebP vulnerability was reported by Apple Security Engineering and Architecture (SEAR) and The Citizen Lab at The University of Toronto's Munk School.

Sept 11, 2023: The Chromium team released the security advisory and fix.
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html

Sept 13, 2023: CISA added Google Chromium WebP Vulnerability (CVE-2023-4863) to its Known Exploited Vulnerabilities Catalog.
https://www.cisa.gov/news-events/alerts/2023/09/13/cisa-adds-three-known-vulnerabilities-catalog

Sept 27, 2023: FortiGuard Labs released a Threat Signal.
https://www.fortiguard.com/threat-signal-report/5260/

Latest Developments

Oct 3, 2023: FortiGuard Labs has released an IPS signature to detect and block any attack attempts targeting to exploit the CVE-2023-4863 vulnerability. It is strongly advised to review vendor advisories and apply their mitigations and updates.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- **Delivery**

Vulnerability

Detects vulnerable application related to Google Chromium WebP Heap-Based Buffer Overflow Vulnerability

FortiClient
DB 1.548

- **Exploitation**

IPS

Detects and blocks attack attempts exploiting Google Chromium WebP Heap-Based Buffer Overflow Vulnerability

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 25.649	*DB 25.649*	*DB 25.649*	*DB 25.649*	*DB 25.649*

Web App Security

Detects and blocks attack attempts exploiting Google Chromium WebP Heap-Based Buffer Overflow Vulnerability

FortiWeb
DB 0.00359

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiClient	FortiAnalyzer
DB 1.00014	*DB 2.00020*

Threat Hunting

FortiAnalyzer
v6.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response	FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training	Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

FortiDevSec

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

Apple	https://support.apple.com/en-us/HT213905
Bleeping Computer	https://www.bleepingcomputer.com/news/google/google-fixes-another-chrome-zero-day-bug-exploited-in-attacks/
Debian	https://security-tracker.debian.org/tracker/CVE-2023-4863
Google	https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
Helpnet Security	https://www.helpnetsecurity.com/2023/09/27/cve-2023-5129/
Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4863
Mozilla	https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/
Ubuntu	https://ubuntu.com/security/CVE-2023-4863

Learn more about FortiGuard Outbreak Alerts