مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Zero-Day in Google Chrome

Tracking #:432319095

Date:09-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released new Chrome Stable Channel for Windows, Mac, and Linux, addressing 74 security fixes, including 17 Critical and 57 High/Medium severity vulnerabilities.

TECHNICAL DETAILS:

Google has released Chrome Stable Channel version 149.0.7827.102/.103 for Windows and macOS and 149.0.7827.102 for Linux. The update contains 74 security fixes, including 17 Critical and 57 High/Medium severity vulnerabilities.
CVE-2026-11645, a High-severity Out-of-Bounds Memory Access vulnerability in the V8 JavaScript engine, for which Google has confirmed active exploitation in the wild.

Actively Exploited Vulnerability

- **CVE-2026-11645**- Severity: High -Out of bounds read and write in V8 in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page

Critical Vulnerability Details:

- CVE-2026-11628 — Critical — Use-after-free in Ozone that could lead to memory corruption, browser crashes, and potential remote code execution.
- CVE-2026-11629 — Critical — Use-after-free in Ozone that may allow an attacker to execute arbitrary code via crafted web content.
- CVE-2026-11630 — Critical — Use-after-free in File Input resulting in memory corruption and possible code execution.
- CVE-2026-11631 — Critical — Use-after-free in Aura that could enable browser compromise through memory corruption.
- CVE-2026-11632 — Critical — Use-after-free in TabStrip leading to browser instability and potential remote code execution.
- CVE-2026-11633 — Critical — Use-after-free in Bluetooth that may permit arbitrary code execution when exploited.
- CVE-2026-11634 — Critical — Use-after-free in Gamepad causing memory corruption and potential browser compromise.
- CVE-2026-11635 — Critical — Use-after-free in Bluetooth that could be leveraged for remote code execution.
- CVE-2026-11636 — Critical — Use-after-free in Autofill allowing memory corruption and potential arbitrary code execution.
- CVE-2026-11637 — Critical — Use-after-free in Views that may result in browser crashes or code execution.
- CVE-2026-11638 — Critical — Use-after-free in Printing leading to memory corruption and potential system compromise.
- CVE-2026-11639 — Critical — Use-after-free in Compositing that could enable arbitrary code execution.
- CVE-2026-11640 — Critical — Integer overflow in libyuv that may lead to memory corruption and potential code execution.
- CVE-2026-11641 — Critical — Use-after-free in Bluetooth that could allow an attacker to execute arbitrary code.

- CVE-2026-11642 — Critical — Use-after-free in Web Apps resulting in memory corruption and possible browser compromise.
- CVE-2026-11643 — Critical — Use-after-free in Proxy that may enable remote code execution.
- CVE-2026-11644 — Critical — Use-after-free in Views leading to memory corruption and potential arbitrary code execution.

Other Notable High-Severity Vulnerabilities

- CVE-2026-11649 / CVE-2026-11650 — High — Use-after-free vulnerabilities in V8 that may result in arbitrary code execution.
- CVE-2026-11662 — High — Type confusion in Bindings that could allow memory corruption and code execution.
- CVE-2026-11667 — High — Out-of-bounds read in WebRTC potentially leading to information disclosure.
- CVE-2026-11672 — High — Out-of-bounds write in GPU leading to memory corruption and potential code execution.
- CVE-2026-11678 — High — Integer overflow in libyuv that may cause memory corruption and application crashes.
- CVE-2026-11690 — High — Out-of-bounds read and write in Media that could result in arbitrary code execution.
- CVE-2026-11698 / CVE-2026-11699 — High — Use-after-free vulnerabilities in Bluetooth that may lead to browser compromise and code execution.

Fixed Versions:

- Windows/macOS: 149.0.7827.102/.103
- Linux: 149.0.7827.102

RECOMMENDATIONS:

Immediate Actions:

- Update Google Chrome to the latest stable version immediately.
- Enable automatic browser updates across enterprise environments.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html