

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



Chrome 102 Update Patches High-Severity Vulnerabilities

By [Ionut Arghire](#) on June 10, 2022

Share

Tweet

推荐 15



Google this week announced the release of a Chrome browser update that resolves seven vulnerabilities, including four issues reported by external researchers.

Tracked as CVE-2022-2007, the first of these bugs is described as a use-after-free in WebGPU. The security hole was reported by David Manouchehri, who received a \$10,000 bug bounty reward for his finding.

Use-after-free issues are triggered when a program doesn't clear the pointer after freeing memory allocation, and can be exploited for arbitrary code execution, denial of service, or data corruption, potentially leading to system compromise, if combined with other vulnerabilities. In the case of Chrome, they often lead to a sandbox escape.

Another use-after-free vulnerability addressed with [this Chrome update](#) is CVE-2022-2011, a flaw identified in ANGLE, Chrome's graphics engine abstraction layer. The bug was reported by SeongHwan Park.

The latest Chrome update also resolves CVE-2022-2008, an out-of-bounds memory access in WebGL, which was reported by VinCSS Cybersecurity researcher Tran Van Khang.

Google says it has yet to determine the bug bounty amounts to be paid for these two vulnerabilities.

The fourth externally reported vulnerability addressed with this browser update is CVE-2022-2010, an out-of-bounds read in compositing, which was reported by Mark Brand of Google Project Zero. As per Google's policies, the researcher won't be awarded a bug bounty.

The latest Chrome iteration is now rolling out to Windows, Mac, and Linux users as version 102.0.5005.115.

Google made no mention of any of these vulnerabilities being exploited in the wild, but users are advised to update their browsers as soon as possible.

Three Chrome vulnerabilities are known to have been [exploited in attacks](#) so far this year.

Related: [Chrome 102 Patches 32 Vulnerabilities](#)

Related: [Chrome 101 Update Patches High-Severity Vulnerabilities](#)

Related: [Chrome 101 Patches 30 Vulnerabilities](#)

[Share](#)[Tweet](#)[推荐 15](#)

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[38 Tech Leaders Sign Cyber Resilience Pledge](#)

[Chinese Cyberspy Group 'Aoqin Dragon' Targeting Southeast Asia, Australia Since 2013](#)

[Chrome 102 Update Patches High-Severity Vulnerabilities](#)

[Highly-Evasive Linux Malware 'Symbiote' Infects All Running Processes](#)

[US Details Chinese Attacks Against Telecoms Providers](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2022 Singapore/APAC ICS Cyber Security Conference](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

Tags:

[NEWS & INDUSTRY](#)

[Vulnerabilities](#)

Search

Get the Daily Briefing

BRIEFING

Business Email Address

Subscribe

