- 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

Google Awards Over $130,000 for Flaws Patched With Release of Chrome 93

By Ionut Arghire on September 01, 2021

Share Tweet Recommend 0 RSS

Google this week announced the release of Chrome 93 with a total of 27 security patches inside, including 19 for vulnerabilities that were reported by external researchers.

A total of five high-severity security bugs addressed with the latest Chrome release were reported externally, all being use-after-free flaws affecting various browser components.

The most severe of these appears to be CVE-2021-30606, a use-after-free in Blink that was reported by 360 Alpha Lab researchers Nan Wang and koocola in late July. Google paid a $20,000 bounty reward for the discovery.

Three other high-severity use-after-free issues were patched in Permissions (CVE-2021-30607), Web Share (CVE-2021-30608), and Sign-In (CVE-2021-30609). Google paid for these vulnerability reports $10,000, $7,500, and $5,000, respectively.

Another high-severity bug addressed with this Chrome release was found in Extensions API. However, Google hasn't issued a reward for the bug as it was reported by someone from browser developer Vivaldi. As per the rules of its Chrome vulnerability reward program, "Chromium embedders and companies with whom Google has a pre-existing business relationship may not be eligible for rewards."

Of the 12 medium-severity flaws patched with this browser iteration, five were use-after-free issues, affecting WebRTC (two security holes), Base internals, Media, and WebApp Installs. Google paid $20,000 for each of the first two and $15,000 for the third bug.

Other medium-severity vulnerabilities included heap buffer overflow, cross-origin data leak, policy bypass, inappropriate implementation, UI spoofing (two bugs), and insufficient policy enforcement.

Two low-severity flaws were patched with the latest Chrome release, both use-after-free issues. Google says it paid a $10,000 reward for the first, but has yet to determine the amount paid for the second.

Overall, Google says it paid over $130,000 in bounty rewards to the reporting researchers.

The latest Chrome iteration is now rolling out to Windows, Mac and Linux users as Chrome 93.0.4577.63.

Related: **Google Awards $42,000 for Two Serious Chrome Vulnerabilities**

Related: **Chrome 92 Brings Several Privacy, Security Improvements**

Related: **Google Adds HTTPS-First Mode to Chrome**

Share Tweet Recommend 0 RSS

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

CISA, FBI Warn of Increase in Ransomware Attacks on Holidays
Singapore Government Launches New Bug Bounty Program
Google Awards Over $130,000 for Flaws Patched With Release of Chrome 93
Proxyware Platforms Increasingly Targeted by Cybercriminals
CISA Expands 'Bad Practices' List With Single-Factor Authentication

sponsored links

Virtual Event Series - Security Summit Online Events by SecurityWeek

2021 ICS Cyber Security Conference | USA [Hybrid: Oct. 25-28]

2021 CISO Forum: September 21-22 - A Virtual Event

2021 Singapore/APAC ICS Cyber Security Conference [Virtual: June 22-24]

Tags:

NEWS & INDUSTRY Vulnerabilities

Search

Get the Daily Briefing

BRIEFING

Business Email Address Subscribe