SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

- 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 Patches Four Severe Vulnerabilities in Chrome

By Ionut Arghire on October 08, 2021

Google this week announced the release of an updated Chrome version for Windows, Mac and Linux, to address a total of four high-severity vulnerabilities in the browser.

Tracked as CVE-2021-37977, the most severe of these security holes could be exploited to achieve arbitrary code execution on a target system.

The flaw, described as a use-after-free bug in Garbage Collection, was reported last month by an anonymous researcher. Google says it paid a $10,000 bounty reward for the finding.

Now rolling out to desktop users as Chrome version 94.0.4606.81, the new browser iteration also addresses two heap buffer overflow vulnerabilities in Blink (CVE-2021-37978) and WebRTC (CVE-2021-37979).

The issues were reported by Yangkang (@dnpushme) of 360 ATA and Marcin Towalski of Cisco Talos, respectively. Google says it handed out $7,500 to each of the reporting researchers.

A fourth high-severity bug addressed with the new Chrome release is CVE-2021-37980, an inappropriate implementation in Sandbox. Yonghwi Jin (@jinmo123), the reporting researcher, received a $3,000 bounty reward for the finding.

Attackers could exploit these vulnerabilities through specially crafted webpages to compromise a visitor's system and potentially execute code in the context of the browser.

Google says the Chrome extended stable channel too was updated to version 94.0.4606.81 for Windows and Mac.

The search giant made no mention of any of these vulnerabilities being exploited in targeted attacks. So far this year, however, there have been more than a dozen documented zero-day exploits targeting the Chrome and Android platforms.

Related: Google Patches Two More Exploited Zero-Day Vulnerabilities in Chrome

Related: Google Warns of Exploited Zero-Days in Chrome Browser

Related: Google Working on Improving Memory Safety in Chrome

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Google Patches Four Severe Vulnerabilities in Chrome
FontOnLake Linux Malware Used in Targeted Attacks
Attackers Encrypt VMware ESXi Server With Python Ransomware
Cisco Patches High-Severity Vulnerabilities in Security Appliances, Business Switches
Nigerian Man Living in U.S. Charged Over Role in BEC Scheme

Tags:

NEWS & INDUSTRY Vulnerabilities

Search

Get the Daily Briefing