- 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

Firefox 102 Patches 19 Vulnerabilities, Improves Privacy

By Ionut Arghire on June 29, 2022

Mozilla this week announced the availability of Firefox 102 in the stable channel with patches for 19 vulnerabilities, including four high-severity bugs.

With the latest update, Mozilla has patched CVE-2022-34470, a high-severity use-after-free issue in nsSHistory that was triggered when navigating between XML documents, and which could lead to a potentially exploitable crash.

Use-after-free vulnerabilities can be exploited to achieve arbitrary code execution, data corruption, or denial of service, and could lead to full system compromise if combined with other flaws. Malicious websites can exploit these bugs to escape a browser's sandbox.

CVE-2022-34468, another high-severity flaw addressed in Firefox 102, could allow for the bypass of a CSP sandbox header without `allow-scripts` by using a retargeted *javascript: URI*. Because of this issue, when a user clicks on a *javascript:* link, an iframe could run scripts without authorization.

The new Firefox release also resolves CVE-2022-34479, a Linux-specific issue that allows malicious websites to create popup windows that can be resized in such a manner that the address bar would be overlayed with web content, potentially leading to spoofing attacks.

Multiple memory safety bugs have been assigned CVE-2022-34484, including ones that "showed evidence of JavaScript prototype or memory corruption and we presume that with enough effort

some of these could have been exploited to run arbitrary code."

Firefox 102 also improves user privacy by mitigating query parameter tracking when navigating the internet with Enhanced Tracking Protection (ETP) strict mode enabled.

With ETP, Firefox confines cookies to the sites that created them, which prevents cross-site tracking. Courtesy of the new capability, Firefox can block specific tracking parameters that websites may be using to circumvent the privacy protections that browsers have implemented.

Additionally, Firefox 102 handles audio decoding in a separate process that features stricter sandboxing, to enhance process isolation.

Related: Emergency Firefox Update Patches Two Actively Exploited Zero-Day Vulnerabilities

Related: New Firefox Feature Ups the Ante Against Cookie-Based Tracking

Related: Google Patches 14 Vulnerabilities With Release of Chrome 103

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Azure Service Fabric Vulnerability Can Lead to Cluster Takeover
Firefox 102 Patches 19 Vulnerabilities, Improves Privacy
CISA Calls for Expedited Adoption of Modern Authentication Ahead of Deadline
CISA-Funded Project Enables Students With Disabilities to Learn Cybersecurity
Google Introduces New Capabilities for Cloud Armor Web Security Service

Tags:
NEWS & INDUSTRY Vulnerabilities