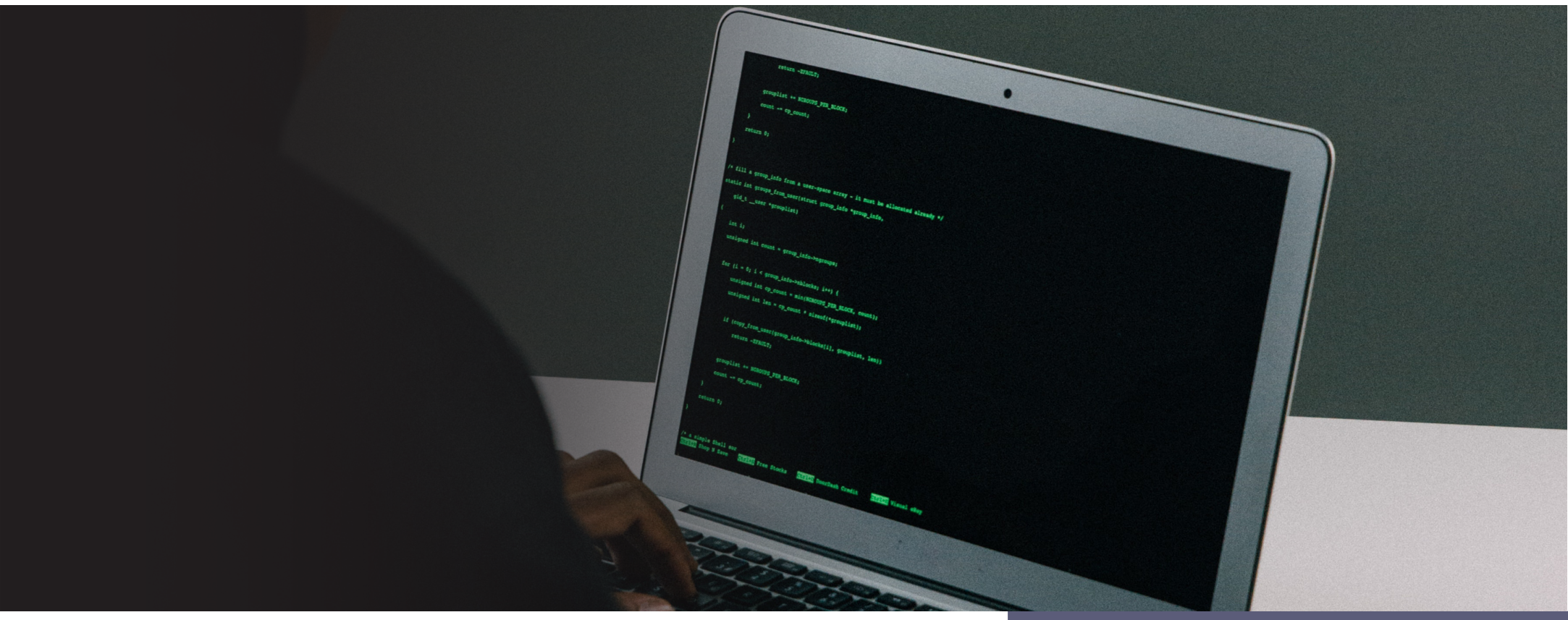
TECH HIVE ADVISORY

Cybersecurity, News, Events and Threat Advisories

Security Advisory

Volume 1 / Issue 3



2021: Zero-Day Attack on the increase

What is the issue

Based on web browsers' usage globally, many users, including businesses, may be at risk. A zero-day flaw may allow attackers to remotely execute codes (install programs, view, change or delete data or create accounts) or cause a denial-of-service attack. A zero-day flaw exploits vulnerability before there is an opportunity to fix same. A consistent vulnerability scanning may not detect all zero-day vulnerabilities and exploits. This vulnerability is reported to affect Windows, macOS, and Linux versions of the browser.

As of March 2021, Google's zero-day tracker spreadsheet has flagged twelve (12) zero-day attacks, which is already half of the total number reported last year. These include the Microsoft Exchange Server vulnerabilities and the SonicWall Enterprise security vulnerability.

What should you do?

- Users who did not set automatic update on their devices are advised to update to the newest version of Chrome rolled out by Google to patch the flaw.
- Organisations should use a solid and effective Web Application Firewall (WAF) to review incoming traffic and filter out malicious ones, thereby preventing vulnerabilities' exploitation.
- Adoption and implementation of an effective incident response plan that includes rehearsed roles and procedures.
- Employees awareness of essential threat identification and mitigation techniques like handling unknown email attachments and suspicious URLs.

As of March 2021, Google's zero-day tracker spreadsheet has flagged twelve (12) zero-day attacks, which is already half of the total number reported last year.

TLDR

A new zero-day vulnerability was reported, which impacts the browser engine, Blink used by most web browsers today- Chrome, Brave, Microsoft Edge etc. Blink converts web page resources into viewable visual representations for users. The specifics of the attack is yet to be disclosed by Google, other than that it is a zero-day flaw (CVE-2021-21193) and a use-after-free flaw- it exploits an accessible memory location whose pointer was not cleared.

See detailed information here.

Severity: high

Contact Us

@techhiveadvisory
contact@techhiveadvisory.org.mg
www.techhiveadvisory.org.ng