**Newly Discovered Zero-Day Attacks**

[Hackers exploit critical flaw in WordPress Royal Elementor plugin](https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-flaw-in-wordpress-royal-elementor-plugin/)(16-10): A critical severity vulnerability impacting Royal Elementor Addons and Templates up to version 1.3.78 is reported to be actively exploited by two WordPress security teams.

Since the exploitation was observed before the vendor released a patch, the flaw was leveraged by hackers as a zero-day.

The flaw impacting the add-on is tracked as CVE-2023-5360 (CVSS v3.1: 9.8 "critical"), allowing unauthenticated attackers to perform arbitrary file uploads on vulnerable sites.

Cisco warns of new IOS XE zero-day actively exploited in attacks(16-10): Cisco warned admins today of a new maximum severity authentication bypass zero-day in its IOS XE software that lets unauthenticated attackers gain full administrator privileges and take complete control of affected routers and switches remotely.

The company says the critical vulnerability (tracked as [CVE-2023-20198](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z) and still waiting for a patch) only affects devices running with the Web User Interface (Web UI) feature enabled, which also have the HTTP or HTTPS Server feature toggled on.

New 'HTTP/2 Rapid Reset' zero-day attack breaks DDoS records(10-10): The novel attack exploits a zero-day vulnerability tracked as CVE-2023-44487, which abuses a weakness in the HTTP/2 protocol.

Simply put, the attack method abuses HTTP/2's stream cancellation feature to continuously send and cancel requests, overwhelming the target server/application and imposing a DoS state.

HTTP/2 features a safeguard in the form of a parameter that limits the number of concurrently active streams to prevent DoS attacks; however, this isn't always effective.

**Radio silence from DMS vendor quartet over XSS zero-days:** The most severe issue belongs to ONLYOFFICE’s Workspace enterprise app platform. Tracked as [CVE-2022-47412](https://www.cve.org/cverecord?id=CVE-2022-47412) and believed to impact versions from 0 through 12.1.0.1760, the [stored cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/stored) (XSS) vulnerability could be exploited if an attacker can ensure a malicious document is saved in the DMS for indexing.

When a victim has unwittingly saved the document and triggered the XSS condition, an attacker could steal session cookies to create new, privileged accounts or perform a browser session hook and secure access to stored documents.

**Researcher drops Lexmark RCE zero-day rather than sell vuln ‘for peanuts’**

A notable and conscientious independent security researcher by the name of Peter Geissler has opted for public disclosure of a zero-day remote code execution (RCE) vulnerability affecting Lexmark printers. He made this decision after deeming the financial reward offered for the vulnerability laughable and inadequate. The RCE vulnerability in question proved to be a significant concern, as it enabled potential compromise of Lexmark printers through seemingly innocuous functions.

**Google Roulette: Developer console trick can trigger XSS in Chromium browsers**

In an intriguing turn of events, security researcher Michał Bentkowski has uncovered a unique case study focusing on cross-site scripting (XSS) attacks within Chromium browsers. These attacks are orchestrated through the utilization of a developer console trick, adding complexity to the realm of browser security. While Chromium browsers boast robust safeguards against XSS attacks, this particular vulnerability stands out due to its challenging nature for exploitation. It is notable that Google has decided not to patch this specific vulnerability, further highlighting the intricate facets of browser security and the ever-evolving tactics employed by malicious actors.

**New DDoS Attack is Record Breaking: HTTP/2 Rapid Reset Zero-Day Reported by Google, AWS & Cloudflare**

A significant security development has come to light, with Google, AWS, and Cloudflare jointly reporting an unprecedented Distributed Denial of Service (DDoS) attack campaign. This campaign is exploiting a recently discovered zero-day vulnerability within the HTTP/2 network protocol, which has been aptly named “HTTP/2 Rapid Reset” and tracked as CVE-2023–44487. This vulnerability, now actively exploited, poses a substantial threat to all organizations and individuals relying on servers that provide HTTP/2 services to the internet. It is worth understanding that HTTP/2 is a vital revision of the HTTP network protocol, designed to enhance the speed, efficiency, and security of web applications.

**Apple fixes iOS Kernel zero-day vulnerability on older iPhones**

Apple has taken proactive measures by releasing security updates for older iPhones and iPads to address two zero-day vulnerabilities that were actively exploited by malicious actors. The first vulnerability, identified as CVE-2023–42824, is a privilege escalation vulnerability resulting from a weakness in the XNU kernel. It had the potential to allow local attackers to elevate their privileges on vulnerable iPhones and iPads. Apple has responded by addressing this vulnerability in iOS 16.7.1 and iPadOS 16.7.1 through improved security checks. The second vulnerability, CVE-2023–5217, was traced to a heap buffer overflow in the VP8 encoding of the open-source libvpx video codec library.