JO-FinCERT – Security Advisory – 2023 – 40

1. Google Issues Patch for New Chrome Vulnerability

Google issued security updates for its Chrome web browser to address a high-severity vulnerability that is currently being actively exploited. The vulnerability, identified as CVE-2023-3079, is categorized as a type of confusion bug within the V8 JavaScript engine.

- **CVE-2023-3079**: Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVSS 9.8/CRITICAL

Reference: https://thehackernews.com/2023/06/zero-day-alert-google-issues-patch-for.html

2. Zyxel Firewalls Under Attack! Urgent Patching Required - Updated

Reference to the Security Advisory-2023-39 article (note below) sent on 4th of June 2023, it has been observed that Zyxel Firewall vulnerabilities are actively being exploited.

Recommendation: Please ensure to apply the patch as per your patching procedure ASAP.

Reference: https://thehackernews.com/2023/06/zyxel-firewalls-under-attack-urgent.html

---

Security Advisory-2023-39

Zyxel shares tips on protecting firewalls from ongoing attacks

Zyxel has recently released a security advisory to provide guidance on safeguarding firewall and VPN devices against ongoing attacks and detecting indicators of exploitation. This advisory is a response to numerous reports highlighting the extensive exploitation of CVE-2023-28771, as well as the concerning exploitability and severity of CVE-2023-33009 and CVE-2023-33010. These vulnerabilities specifically impact Zyxel's VPN and firewall devices.

- **CVE-2023-28771:** allow an unauthenticated attacker to execute some OS commands remotely by sending crafted packets to an affected device. CVSS 9.8/CRITICAL
- **CVE-2023-33009:** allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and even a remote code execution on an affected device. CVSS 9.8/CRITICAL

- **CVE-2023-33010:** allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and even a remote code execution on an affected device. CVSS 9.8/CRITICAL

Recommendation: Financial entities are required to apply vendor's updates as per patch management procedure.

Reference: https://www.bleepingcomputer.com/news/security/zyxel-shares-tips-on-protecting-firewalls-from-ongoing-attacks/