JO-FinCERT – Security Advisory – 2023 – 45

1. MOVEit Transfer customers warned of new flaw as PoC info surfaces

Progress has issued a security warning to its MOVEit Transfer customers regarding a newly discovered SQL injection (SQLi) flaw, identified as CVE-2023-35708. This critical vulnerability could lead to unauthorized access and escalated privileges within affected environments. Progress has released security patches for all affected software versions to address the issue and advises customers to restrict HTTP access and apply the provided patch promptly. As a precaution, both Progress and customers are recommended to temporarily disable HTTP and HTTPS traffic on ports 80 and 443. Although web UI access may be affected, file transfers can still be conducted using SFTP and FTP/s protocols. Administrators can access MOVEit Transfer through a remote desktop and by visiting "https://localhost/" on the Windows server.

1. **CVE-2023-35708:** an attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content.

Reference:https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

2. Western Digital boots outdated NAS devices off of My Cloud

Western Digital has issued a warning to owners of My Cloud series devices, stating that starting from June 15, 2023, devices that are not upgraded to the latest firmware version 5.26.202 will no longer be able to connect to Western Digital cloud services. This action is taken to protect users from a remotely exploitable vulnerability that can lead to unauthenticated code execution. The firmware update addresses critical security flaws, including path traversal, uncontrolled resource consumption, authentication bypass, and server-side request forgery vulnerabilities. Failure to update the firmware may result in unauthorized access to devices, data breaches, and potential ransomware attacks. The affected devices include various models of My Cloud, My Cloud Home, My Cloud EX, and My Cloud Mirror. Users are advised to update their devices to the specified firmware versions to ensure continued access to cloud services and mitigate the risk of cyberattacks.

1. **CVE-2022-36327:** path traversal flaw allowing an attacker to write files to arbitrary filesystem locations, leading to unauthenticated (authentication bypass) remote code execution on My Cloud devices. 9.8 / (CRITICAL)
2. **CVE-2022-36326**: Uncontrolled resource consumption issue triggered by specially crafted requests sent to vulnerable devices, causing DoS. 4.9 / (MEDIUM)

JO-FinCERT – Security Advisory – 2023 – 45

3. **CVE-2022-36328:** Path traversal flaw allowing an authenticated attacker to create arbitrary shares on arbitrary directories and exfiltrate sensitive files, passwords, users, and device configurations. 4.9 / (MEDIUM)
4. **CVE-2022-29840:** Server-Side Request Forgery (SSRF) vulnerability that could allow a rogue server on the local network to modify its URL to point back to the loopback. 5.5 / (MEDIUM)

Reference:https://www.bleepingcomputer.com/news/security/western-digital-boots-outdated-nas-devices-off-of-my-cloud/