مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Pre-Auth RCE Vulnerabilities in SysAid On-Premise Software

Tracking #:432317233

Date:08-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers have identified four critical vulnerabilities in SysAid On-Premise IT support software, three of which are XML External Entity (XXE) injection flaws that can be exploited without authentication, potentially leading to Remote Code Execution (RCE).

TECHNICAL DETAILS:

Security researchers have identified four critical vulnerabilities in SysAid On-Premise IT support software, three of which are XML External Entity (XXE) injection flaws that can be exploited without authentication, potentially leading to Remote Code Execution (RCE). SysAid vulnerabilities have historically been targeted in real-world attacks. Notably, CVE-2023-47246 was previously exploited by Cl0p ransomware operators in zero-day campaigns. With the availability of a PoC exploit for the newly disclosed 2025 flaws, the threat level is elevated, especially for organizations with exposed or unpatched instances.

Vulnerability Details:

CVE-ID	Vulnerability Type	Endpoint	Authentication Required	Impact
CVE-2025-2775	XML External Entity Injection (XXE)	/mdm/checkin	No	File Disclosure, SSRF
CVE-2025-2776	XML External Entity Injection (XXE)	/mdm/checkin	No	File Disclosure, SSRF
CVE-2025-2777	XML External Entity Injection (XXE)	/lshw	No	File Disclosure, SSRF
CVE-2025-2778	OS Command Injection	Unspecified	Requires chaining	Remote Code Execution

- Fixed Version:**24.4.60 b16**

RECOMMENDATIONS:

- Upgrade SysAid On-Premise to fixed version or later without delay.
- Conduct a forensic review of SysAid systems for signs of unauthorized access or exploitation.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://documentation.sysaid.com/docs/24-40-60