مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Critical Vulnerabilities in Cacti

Tracking #:432319218

Date:30-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities have been identified in Cacti, a widely used open-source network monitoring and graphing platform.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified in Cacti, a widely used open-source network monitoring and graphing platform. The vulnerabilities include three pre-authentication SQL Injection flaws and one unauthenticated Local File Inclusion (LFI) vulnerability. Successful exploitation could allow attackers to access or manipulate the Cacti database, disclose sensitive information, or read arbitrary files from the underlying server.

Vulnerability Details:

- CVE-2026-39893 – Pre-Authentication SQL Injection (CWE-89) – CVSS 9.8
- CVE-2026-39955 – Pre-Authentication SQL Injection (CWE-89) – CVSS 9.8
- CVE-2026-39948 – SQL Injection via rfilter Parameter (RLIKE Clause) – CVSS 9.3
- CVE-2026-39938 – Local File Inclusion (Path Traversal) (CWE-22) – CVSS 9.8

Affected Versions

- Cacti 1.2.30 and earlier

Patched Version

- Cacti 1.2.31

RECOMMENDATIONS:

Immediate Actions:

- Organizations should prioritize upgrading Cacti to fixed version and implement recommended mitigations to reduce the risk of compromise.

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://github.com/Cacti/cacti/releases/tag/release%2F1.2.31