مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in Cacti

Tracking #:432316787

Date:27-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Cacti, a PHP-based network monitoring tool, that allows authenticated users to execute arbitrary system commands on the server.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-22604) has been discovered in Cacti, a PHP-based network monitoring tool, that allows authenticated users to execute arbitrary system commands on the server. This vulnerability arises due to improper handling of multi-line SNMP responses when parsing Object Identifiers (OIDs), enabling an attacker to inject and execute malicious code.

- CVE ID: **CVE-2025-22604**
- Vulnerability Type: Remote Code Execution (RCE)
- CVSS Severity: Critical,9.1/10
- Vulnerable Software: Cacti (PHP-based version)
- Affected Versions: <= 1.2.8
- Patched Version: 1.2.29 and above
- CWE Classification: CWE-78: Improper Neutralization of Special Elements used in an OS Command

RECOMMENDATIONS:

- Upgrade Cacti to version 1.2.29 or later immediately.
- Implement network segmentation to limit access to Cacti instances.
- Enforce strong authentication mechanisms and principle of least privilege.
- Monitor Cacti systems for suspicious activities or unauthorized changes.

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/security/advisories/GHSA-c5j8-jxj3-hh36