



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- Cacti Framework Critical Vulnerabilities

Tracking #:432315857

Date:15-05-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in the Cacti open-source network monitoring and fault management framework, which could be exploited to execute arbitrary code on the underlying server, potentially leading to complete system compromise.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-25641 (CVSS score: 9.1 Critical):** This vulnerability exists in the "Package Import" feature and allows authenticated users with "Import Templates" permission to upload a malicious package containing PHP code. This code can then be executed on the server, potentially leading to complete system compromise.
- **CVE-2024-29895 (CVSS score: 10.0 Critical):** This unauthenticated command injection vulnerability allows any attacker to execute arbitrary commands on the server if the "register_argc_argv" option in PHP is enabled. This could be exploited to gain unauthorized access to the system, steal data, or deploy malware.
- **CVE-2024-31445 (CVSS score: 8.8 High):** An SQL injection vulnerability that could allow authenticated users to escalate privileges and execute code.
- **CVE-2024-31459 (High):** A file inclusion vulnerability that could be chained with SQL injection to achieve remote code execution.

Affected Versions:

- All versions of Cacti prior to 1.2.27

Fixed Versions:

- Cacti 1.2.27 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the latest fixed version released by Cacti.

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-7cmj-g5qc-pj88>
- <https://github.com/Cacti/cacti/security/advisories/GHSA-cr28-x256-xf5m>
- <https://github.com/cacti/cacti/security/advisories/GHSA-vjph-r677-6pcc>
- <https://github.com/cacti/cacti/security/advisories/GHSA-cx8g-hvq8-p2rv>