مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Command Injection Vulnerability in Webmin

Tracking #:432316666

Date:25-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability in Webmin, the popular web-based system administration tool, which could potentially be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-12828**
- CVSS Score: 9.9 (Critical)
- The vulnerability stems from improper sanitization of user-supplied input in Webmin's CGI request handling. Authenticated attackers, including those with lower privileges, can exploit this flaw to inject and execute arbitrary commands with root privileges
- Successful exploitation of this vulnerability can have severe consequences, including full server compromise, unauthorized access to sensitive data, deployment of malicious scripts and ransomware, and the use of compromised servers for further attacks.

Affected Versions:

- Webmin versions prior to 2.111

Fixed Versions:

- Webmin version 2.111 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://www.zerodayinitiative.com/advisories/ZDI-24-1725/
- https://webmin.com/security/#privilege-escalation-by-non-root-users-cve-2024-12828