مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates – Ubuntu OpenVPN

Tracking #:432316110

Date:02-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Canonical released security updates to address multiple vulnerabilities in OpenVPN, a virtual private network software.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-28882**
  - It was found that OpenVPN in a server role accepts multiple exit notifications from authenticated clients.
  - This oversight allows a remote authenticated client to keep the connection active and extend the validity of a closing session.
  - This vulnerability only affected Ubuntu 23.10, and Ubuntu 24.04 LTS.

- **CVE-2024-5594**
  - This vulnerability involves the incorrect handling of certain control channel messages with nonprintable characters.
  - A remote attacker could possibly use this issue to cause OpenVPN to cause high CPU load, or fill up log files with garbage, leading to a denial of service.

Fixed Versions:

- Ubuntu 24.04: 2.6.9, Ubuntu 23.10: 2.6.5 Ubuntu 22.04: 2.5.9, Ubuntu 20.04: 2.4.12

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Canonical.

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://ubuntu.com/security/CVE-2024-28882
- https://ubuntu.com/security/CVE-2024-5594