Multiple Vulnerabilities in OpenVPN

Severity Level: Medium

Components Affected

OpenVPN Access Server versions 2.11.0, 2.11.1, 2.11.2, 2.11.3, 2.12.0, and 2.12.1

Overview

Multiple vulnerabilities were identified in OpenVPN. A remote attacker could exploit some of these vulnerabilities to trigger denial of service condition and sensitive information disclosure on the targeted system.

Description

Two vulnerabilities have been discovered in OpenVPN. The first involves a division by zero crash, which is less easily exploitable on Access Server due to its default configuration not including the --fragment option and enhanced control channel security. However, under specific circumstances, exploitation is still possible. The second vulnerability is a more serious use after free memory security issue, posing a risk of leaking sensitive information from memory. This vulnerability arises from OpenVPN incorrectly utilizing a freed send buffer, potentially disclosing information to the client peer. The TLS configuration is affected by this vulnerability.

Impact

- Denial of Service
- Information Disclosure

Solution/ Workarounds

Apply fixes issued by the vendor:

https://openvpn.net/security-advisory/access-server-security-update-cve-2023-46849-cve-2023-46850/

Reference

https://www.hkcert.org/security-bulletin/openvpn-multiple-vulnerabilities_20231114

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.