


## Alert Bulletin

**Bulletin N.:** 2024-28

**Publication Date:** 10/09/2024

**Subject:** Alert 2024-28 Critical Vulnerability in SonicWall Exploited by Akira Ransomware Actors

**Traffic Light Protocol (TLP):** White



A critical vulnerability, identified as **CVE-2024-40766** with a CVSS score of **9.3**, was disclosed by **SonicWall**, affecting their firewalls running **SonicOS** in generations 5, 6, and some versions of 7. This vulnerability arises from improper access control to the SonicOS management interface and SSLVPN functionality. The flaw allows attackers to gain unauthorized access to resources or cause the firewall to crash.

The **Akira ransomware actors** have been actively exploiting this vulnerability as an initial access vector, compromising local **SSLVPN user accounts**, especially when **Multi-Factor Authentication (MFA)** is disabled.

Recently, active exploitation of this vulnerability has been observed in several organizations in **Mexico**, making it urgent to take immediate action.