SonicWall Vulnerability

SonicWall has identified a post-authentication stack-based buffer overflow vulnerability that can lead to a firewall crash. This allows a malicious actor to send a malicious request with a specially crafted URL to create a Denial of Service (DoS) attack that may cause the firewall to crash.

SonicWall has rated this a 7.7 out of 10 on the CVSS (Common Vulnerability Scoring System).

SonicWall recommends an immediate upgrade to the latest firmware version on all devices that have this vulnerability. Given the severity of this vulnerability, we will begin updating SonicWall firewalls in use by our recurring service customers, beginning this evening. It is expected that the firmware upgrade should not exceed one half hour per device.

Further information regarding this vulnerability is available on the SonicWall website via the links provided below. Should you have questions or desire confirmation that your specific environment has been updated or is slated for updating, you may respond to this email or contact our support helpdesk at 424-207- 5140.

- Security Advisory (sonicwall.com)
- Stack-Based Buffer Overflow and SonicOS SSL VPN Tunnel Vulnerability | SonicWall

Sincerely,

Chris Harper
Chief Security Officer
Sandbox Technologies, Inc.