UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00233

SONICWALL VPN CRITICAL BUGS ALLOWS FULL TAKEOVER

DATE ISSUED: 14th December 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Sonicwall's Secure Mobile Access (SMA) 100-series VPN appliance are vulnerable to a new set of bugs by which attackers are able to gain root-level access for full device takeover. The most severe of the bugs carries a 9.8 rating on the CVSS scale.

BREAKDOWN

The most critical vulnerability (CVE-2021-20038) would allow a remote, unauthenticated attacker to gain access to the appliance as root and execute code as a "nobody" user giving them full control over the device. They would then be free to alter, enable or disable policies, user account and applications as they wish. This is possible due to the mishandling of environment variables from the HTTP GET method in the appliances httpd server. Additional vulnerabilities include CVE-2021-20038, CVE-2021-20045 (9.4 CVSS) which are file explorer heap and stack-based buffer overflow which have the potential to allow for Remote Code Execution (RCE) as root. CVE-2021-20043 (8.8 CVSS) is also a heap-based buffer overflow attack, however an attacker would need to be an authenticated user to carry out RCE. Further vulnerabilities include:

- CVE-2021-20039 Authenticated command injection
- CVE-2021-20040 Unauthenticated file upload path traversal
- CVE-2021-20041 Unauthenticated CPU exhaustion
- CVE-2021-20042 Unauthenticated Confused Deputy
- CVE-2021-20044 Post-authentication remote command injection

REMEDIATION STEPS

- Apply all security patches issued by SonicWall.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/critical-sonicwall-vpn-bugs-appliance-takeover/176869/