NCSC
National Cyber Security Centre

2112091207-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Multiple Vulnerabilities Patched in SonicWall SMA100 Series
2021-12-09

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

SonicWall has released patches to address critical and medium severity vulnerabilities (CVSS 5.3-9.8) in the SMA 100 series application. The full advisory from SonicWall can be found here. **Note:** There is no evidence that these vulnerabilities are being exploited in the wild.

The NCSC recommends that affected organisations patch related products to ensure security of the devices. The two highest ranked vulnerabilities are listed below, please check the SonicWall site for a full list of patched vulnerabilities.

- **SMA-3217 - SMA100 Unauthenticated Stack-based buffer overflow (CVSS 9.8)**
  - A critical severity vulnerability (CVSS 9.8) in SMA 100 appliances, which includes SMA 200, 210, 400, 410 and 500v could allow a remote unauthenticated attacker to cause Stack-based Buffer Overflow and would result in code execution as the nobody user in the SMA100 appliance. It was noticed that the SMA 100 users with licensed/enabled WAF are impacted by this vulnerability.
- **SMA-3235 - Multiple SMA 100 Unauthenticated File Explorer Heap-based and Stack-based Buffer Overflows (CVSS 9.4)**
  - A critical severity vulnerability (CVSS 9.4) in SMA 100 appliances, which includes SMA 200, 210, 400, 410 and 500v could allow a remote unauthenticated attacker to cause Heap-based and Stack-based Buffer Overflow and would result in code execution as the nobody user in the SMA100 appliance. It was observed that the SMA100 appliances with WAF licensed/enabled are also impacted by this vulnerability. Exploitation potentially leading to code execution.

Impact

A remote authenticated attacker can execute arbitrary commands.

Recommendations

The NCSC recommends that affected organisations review the SonicWall Advisory and apply patches as soon as possible.

DISCLAIMER: *This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie