National Cyber Security Centre

2109241231-NCSC

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

# NCSC Alert

## SonicWall Vulnerability in SMA 100 Series Appliances
## 2021-09-24

**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

A Critical Arbitrary File Delete Vulnerability exists in SonicWall SMA 100 Series Appliances, which include SMA 200, 210, 400, 410 and 500v. The vulnerability SNWLID-2021-0021 could potentially allow a remote unauthenticated attacker the ability to delete arbitrary files from a vulnerable device, potentially gaining administrator access to the underlying host. This is due to improper limitation of a file path to a restricted directory.

## Products Affected

- 9.0.0.10-28sv and earlier
- 10.2.0.7-34sv and earlier
- 10.2.1.0-17sv and earlier

## Impact

Adminstrator access to underlying host - compromised systems, data loss.

## Recommendations

The NCSC recommends that affected organisations review the SonicWall Notification and login to their respective MySonicWall Accounts to upgrade their appliances to the patched versions of firmware. Further information on how to upgrade the firmware can be found in the following KB article. .

**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