National Cyber Security Centre

2101251005-NCSC

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

NCSC Flash Alert

SonicWall Vulnerability
2021-01-25

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.*

Threat Type	The NCSC has received information that a coordinated attack has occured on cybersecurity provider, SonicWall's internal systems, by sophisticated threat actors exploiting possible zero-day vulnerabilities in specific SonicWall secure remote access products. Please review SonicWall's updated product notification here.
Products Affected	At the time of writing, the SMA 100 Series remains under investigation for vulnerability exploitation.
Impact	Compromised Information Systems.
Recommendations	SonicWall advise SMA 100 series administrators to: • Create specific access rules or disable Virtual Office and HTTPS administrative access from the Internet while they continue to investigate the vulnerability. • Enable Multifactor Authentication on all SonicWall SMA, Firewall and MySonicWall Accounts. Ref: 1, 2, 3. • Enable logging and remain vigilant for anonymous or unusual activity on your SonicWall products. • Monitor SonicWall's securty notifications for updates, software patches or updated mitigation actions.

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