An official website of the United States government   Here's how you know ∨

Ransomware Risk in Unpatched, EOL SonicWall SRA and SMA 8.x Products

Original release date: July 15, 2021

CISA is aware of threat actors actively targeting a known, previously patched, vulnerability in SonicWall Secure Mobile Access (SMA) 100 series and Secure Remote Access (SRA) products running unpatched and end-of-life (EOL) 8.x firmware. Threat actors can exploit this vulnerability to initiate a targeted ransomware attack.

CISA encourages users and administrators to review the SonicWall security advisory and upgrade to the newest firmware or disconnect EOL appliances as soon as possible. Review the CISA Bad Practices webpage to learn more about bad cybersecurity practices, such as using EOL software, that are especially dangerous for organizations supporting designated Critical Infrastructure or National Critical Functions.

This product is provided subject to this Notification and this Privacy & Use policy.