Customer Notice

October 22, 2020

RE: "SonicWall DoS & XSS Vulnerabilities"

Dear Hitachi Customer:

Your Hitachi MRI and/or CT product utilizes a SonicWall firewall to augment the cyber security of your device. Hitachi provides and maintains these Sonicwall units as part of your contract with Hitachi.

On October 21, 2020, Sonicwall released a Security Advisory detailing 11 unique vulnerabilities in their firewall products. Details can be found here:

https://www.sonicwall.com/support/product-notification/sonicwall-dos-xss-vulnerabilities

The affected Sonicwall models in use by Hitachi, and their patch version:

TZ-100	will be patched to v5.9.2.13-7o
TZ-105	will be patched to v5.9.2.13-7o
SOHO	will be patched to v5.9.2.13-7o
SOHO-250	will be patched to v6.5.4.7-83n

Hitachi will be patching the Sonicwall software for all contract & warranty customers. This patch will mitigate the vulnerabilities in the Sonicwall. No action is required on your part. Your service engineer will be contacting you to complete a Service Bulletin (SIB 222) to update the Sonicwall Hitachi has installed on your modality computer.

The following is a summary of 11 CVEs published by SonicWall PSIRT :

CVE-2020-5133 & CVE-2020-5135: : Allow unauthenticated/authenticated attacker to cause Denial of Service (Dos) due to buffer overflow, which leads to a firewall crash.
CVE-2020-5134: Out-of-bound invalid file reference condition allows remote attacker to crash the firewall.
CVE-2020-5136 & CVE-2020-5137: Using firewall SSL-VPN port, an unauthenticated/authenticated attacker can cause Denial of Service (DoS), which may lead to firewall crash.
CVE-2020-5138: Heap overflow allows remote attacker to crash firewall using firewall SSL-VPN port.
CVE-2020-5139: Release of invalid pointer condition allows remote attacker to cause Denial of Service (DoS) attack against firewall.
CVE-2020-5140: Memory address leak in the HTTP server response; condition allows remote attacker to cause Denial of Service (DoS) attack against firewall.
CVE-2020-5141: Allows unauthenticated remote attacker to brute force Virtual Assist ticket ID.
CVE-2020-5142: Cross-site-scripting (XSS) vulnerability in the SSL-VPN portal.
CVE-2020-5143: Allows User Enumeration; it is possible to enumerate firewall administrator username based on the login error message displayed on the SSL-VPN login page.

If you have any questions on this matter, please contact Hitachi Regulatory Affairs at QualityRecords@hitachihealthcare.com .