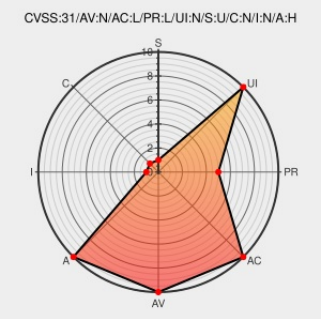
CVE-2019-7474

Published on: 04/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:51 PM UTC

CVE-2019-7474

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Sonicos from Sonicwall contain the following vulnerability:

A vulnerability in SonicWall SonicOS and SonicOSv, allow authenticated read-only admin to leave the firewall in an unstable state by downloading certificate with specific extension. This vulnerability affected SonicOS Gen 5 version 5.9.1.10 and earlier, Gen 6 version 6.2.7.3, 6.5.1.3, 6.5.2.2, 6.5.3.1, 6.2.7.8, 6.4.0.0, 6.5.1.8, 6.0.5.3-86o and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V).

CVE-2019-7474 has been assigned by PSIRT@sonicwall.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Security Advisory	Vendor Advisory	CONFIRM psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0001

Security Advisory	Vendor Advisory psirt.global.sonicwall.com text/html	CONFIRM psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0001

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sonicwall	Sonicos	6.0.5.3-86o	All	All	All
Operating System	Sonicwall	Sonicos	6.2.7.3	All	All	All
Operating System	Sonicwall	Sonicos	6.2.7.8	All	All	All
Operating System	Sonicwall	Sonicos	6.4.0.0	All	All	All
Operating System	Sonicwall	Sonicos	6.5.1.3	All	All	All
Operating System	Sonicwall	Sonicos	6.5.1.8	All	All	All
Operating System	Sonicwall	Sonicos	6.5.2.2	All	All	All
Operating System	Sonicwall	Sonicos	6.5.3.1	All	All	All
Operating System	Sonicwall	Sonicos	6.0.5.3-86o	All	All	All
Operating System	Sonicwall	Sonicos	6.2.7.3	All	All	All
Operating System	Sonicwall	Sonicos	6.2.7.8	All	All	All
Operating System	Sonicwall	Sonicos	6.4.0.0	All	All	All
Operating System	Sonicwall	Sonicos	6.5.1.3	All	All	All
Operating System	Sonicwall	Sonicos	6.5.1.8	All	All	All
Operating System	Sonicwall	Sonicos	6.5.2.2	All	All	All
Operating System	Sonicwall	Sonicos	6.5.3.1	All	All	All
Operating System	Sonicwall	Sonicos	All	All	All	All

Operating System	Sonicwall	Sonicosv	6.5.0.2-8v_rc363	All	All	All
Operating System	Sonicwall	Sonicosv	6.5.0.2.8v_rc366	All	All	All
Operating System	Sonicwall	Sonicosv	6.5.0.2.8v_rc367	All	All	All
Operating System	Sonicwall	Sonicosv	6.5.0.2.8v_rc368	All	All	All
Operating System	Sonicwall	Sonicosv	6.5.0.2-8v_rc363	All	All	All
Operating System	Sonicwall	Sonicosv	6.5.0.2.8v_rc366	All	All	All
Operating System	Sonicwall	Sonicosv	6.5.0.2.8v_rc367	All	All	All
Operating System	Sonicwall	Sonicosv	6.5.0.2.8v_rc368	All	All	All

cpe:2.3:o:sonicwall:sonicos:6.0.5.3-86o:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.2.7.3:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.2.7.8:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.4.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.1.8:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.0.5.3-86o:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.2.7.3:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.2.7.8:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.4.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.1.8:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:6.5.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2-8v_rc363:*:*:*:*:vmware:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2.8v_rc366:*:*:*:*:hyper_v:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2.8v_rc367:*:*:*:*:azure:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2.8v_rc368:*:*:*:*:aws:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2-8v_rc363:*:*:*:*:vmware:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2.8v_rc366:*:*:*:*:hyper_v:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2.8v_rc367:*:*:*:*:azure:*:*:

cpe:2.3:o:sonicwall:sonicosv:6.5.0.2.8v_rc368:*:*:*:*:aws:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→