Hive Pro

THREAT ADVISORY

UNC2682 behind the Zero-day Exploit on SonicWall

TA202108

Threat Level Red

Publish Date – April 22, 2021

UNC2682 is using 3 formerly unknown vulnerabilities of the SonicWall Email services to get authenticated access(CVE-2021-20021), read files (CVE-2021-20022), and modify file(CVE-2021-20023). A Behinder Webshell is planted in the already existing Tomcat Java web server to gain additional information about the Network. These Vulnerabilities can move laterally infecting the whole organization. However, these vulnerabilities can be used in various ways to accomplish targets.
Sonic wall has released patches for all 3 vulnerabilities and applied the following IPS Signatures in all their active subscriptions:

- IPS Signature: 15520 WEB-ATTACKS SonicWall Email Security (CVE-2021-20022 Vulnerability)
- IPS Signature: 1067 WEB-ATTACKS Web Application Directory Traversal Attack 7
- IPS Signature: 15509 WEB-ATTACKS Web Application Directory Traversal Attack 7 -c2

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-20021	SonicWall Email Security version 10.0.9.x	cpe:2.3:a:sonicwall:email_security:*:*:*:*:*:*:*:* cpe:2.3:a:sonicwall:hosted_email_security:*:*:*:*:*:*:*:*	Email Security Pre-Authentication Administrative Account Creation	CWE-269
CVE-2021-20022			Email Security Post-Authentication Arbitrary File Creation	CWE-434
CVE-2021-20023			Email Security Post-Authentication Arbitrary File Read	CWE-22

Patch Links

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0007
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0008
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0010

References

https://thehackernews.com/2021/04/3-zero-day-exploits-hit-sonicwall.html
https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/
https://www.scmagazine.com/home/email-security/someone-is-using-sonicwalls-email-security-tool-to-hack-customers/
https://www.fireeye.com/blog/threat-research/2021/04/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise.html
https://www.bleepingcomputer.com/news/security/sonicwall-warns-customers-to-patch-3-zero-days-exploited-in-the-wild/