CISA warns orgs of WatchGuard bug exploited by Russian state hackers

bleepingcomputer.com/news/security/cisa-warns-orgs-of-watchguard-bug-exploited-by-russian-state-hackers/

Sergiu Gatlan

By
Sergiu Gatlan

- April 11, 2022
- 06:24 PM
- 0

The Cybersecurity and Infrastructure Security Agency (CISA) has ordered federal civilian agencies and urged all US organizations on Monday to patch an actively exploited bug impacting WatchGuard Firebox and XTM firewall appliances.

Sandworm, a Russian-sponsored hacking group, believed to be part of the GRU Russian military intelligence agency, also exploited this high severity privilege escalation flaw (CVE-2022-23176) to build a new botnet dubbed Cyclops Blink out of compromised WatchGuard Small Office/Home Office (SOHO) network devices.

"WatchGuard Firebox and XTM appliances allow a remote attacker with unprivileged credentials to access the system with a privileged management session via exposed management access," the company explains in a security advisory rating the bug with a critical threat level.

The flaw can only be exploited if they are configured to allow unrestricted management access from the Internet. By default, all WatchGuard appliances are configured for restricted management access.

Federal Civilian Executive Branch Agencies (FCEB) agencies must secure their systems against these security flaws according to November's binding operational directive (BOD 22-01).

CISA has given them three weeks, until May 2nd, to patch the CVE-2022-23176 flaw added today to its catalog of Known Exploited Vulnerabilities.

Even though this directive only applies to federal agencies, CISA also strongly urged all US organizations to prioritize fixing this actively abused security bug to avoid having their WatchGuard appliances compromised.

Malware hit 1% of WatchGuard firewall appliances

Cyclops Blink, the malware used by the Sandworm state hackers to create their botnet, has been used to target WatchGuard Firebox firewall appliances with CVE-2022-23176 exploits, as well as multiple ASUS router models, since at least June 2019.

It establishes persistence on the device through firmware updates, and it provides its operators with remote access to compromised networks.

It uses the infected devices' legitimate firmware update channels to maintain access to the compromised devices by injecting malicious code and deploying repacked firmware images.

This malware is also modular, making it simple to upgrade and target new devices and security vulnerabilities, tapping into new pools of exploitable hardware.

WatchGuard issued its own advisory after US and UK cybersecurity and law enforcement agencies linked the malware to the GRU hackers, saying that Cyclops Blink may have hit roughly 1% of all active WatchGuard firewall appliances.

The UK NCSC, FBI, CISA, and NSA joint advisory says organizations should assume all accounts on infected devices as being compromised. Admins should also immediately remove Internet access to the management interface.

Botnet disrupted, malware removed from C2 servers

On Wednesday, US government officials announced the disruption of the Cyclops Blink botnet before being weaponized and used in attacks.

The FBI also removed the malware from Watchguard devices identified as being used as command and control servers, notifying owners of compromised devices in the United States and abroad before cleaning the Cyclops Blink infection.

"I should caution that as we move forward, any Firebox devices that acted as bots, may still remain vulnerable in the future until mitigated by their owners," FBI Director Chris Wray warned.

"So those owners should still go ahead and adopt Watchguard's detection and remediation steps as soon as possible."

WatchGuard has shared instructions on restoring infected Firebox appliances to a clean state and updating them to the latest Fireware OS version to prevent future infections.

Related Articles:

CISA adds 41 vulnerabilities to list of bugs used in cyberattacks

CISA warns admins to patch actively exploited Spring, Zyxel bugs

CISA shares guidance to block ongoing F5 BIG-IP attacks

CISA tells federal agencies to fix actively exploited F5 BIG-IP bug

US offers $10 million reward for tips on Russian Sandworm hackers