HC3: Sector Alert

August 19, 2021 TLP: White Report: 202108191700

FORTIWEB ZERO-DAY VULNERABILITY

Executive Summary

A zero-day command injection vulnerability has been identified in Fortinet's FortiWeb web application firewall (WAF) and effects versions 6.3.11 and earlier. This OS Command injection vulnerability allows remote, authenticated attackers, to execute arbitrary commands on the system through the SAML server configuration page allowing for full compromise of the system and the potential for further compromise of the enterprise network. Fortinet will be releasing a patch on or about August 20, 2021 which is intended to fix this vulnerability. HC3 recommends all HPH sector entities test and apply the FortiWeb Firewall patch to any vulnerable system as soon as it becomes available.

Report

A researcher recently reported the FortiWeb WAF zero-day vulnerability, which has yet to receive a CVE ID, that impacts Fortinet FortiWeb versions 6.3.11 and earlier. The OS Command injection vulnerability in FortiWeb's management interface allows an authenticated attacker to execute arbitrary commands as the root user on the underlying system via the SAML server configuration page remotely. This is an instance of CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') and has a CVSSv3 base score of 8.7. This vulnerability is related to CVE-2021-22123, which was addressed in FG-IR-20-120.

The attacker can use this vulnerability to completely control the targeted device, acquiring the highest system privileges possible. Additionally, the attacker has the ability to install additional malware such as a persistent shell or disruptive or data theft capabilities potentially able to significantly harm a healthcare organization. Although attackers must be authenticated through the management interface of FortiWeb's targeted device to abuse this vulnerability, the attacker can easily chain this attack with other vulnerabilities such as the CVE-2020-29015 authentication bypass to also gain complete control of vulnerable servers.

Unpatched Fortinet servers have been historically targeted by financially motivated criminals and state-sponsored actors, both of whom have a long history of attacking the health sector.

Patches, Mitigations, and Workarounds

HC3 recommends anyone using Fortinet's FortiWeb Firewall apply the patch FortiWeb 6.4.1 to any vulnerable system immediately upon its publication on or around August 19, 2021, which is the rough projected release date by Fortinet. HC3 has also included a list of additional FortiWeb Vulnerabilities in this report. It is also recommended that administrators block access to the FortiWeb device's management interface from untrusted networks (i.e., the Internet) to proactively prevent or defend against attacks or threat actors that would try to exploit this bug until the patch is available. Devices should only be reachable either via trusted, internal networks and always via a secure connection such as a virtual private network to block threat actors' exploitation attempts.

HC3: Sector Alert

August 19, 2021 TLP: White Report: 202108191700

Vulnerabilities

Further details on the Fortinet WAF vulnerability can be found below:

CVE-2021-22123	78	Exec Code	2021-06-01	2021-06-10	9.0	None	Remote	Low	???	Complete	Complete	Complete
An OS command injection vulnerability in FortiWeb's management interface 6.3.7 and below, 6.2.3 and below, 6.1.x, 6.0.x, 5.9.x may allow a remote authenticated attacker to execute arbitrary commands on the system via the SAML server configuration page.												

References

FortiWeb - OS command injection vulnerability
https://www.fortiguard.com/psirt/FG-IR-20-120

CVE Details: Fortinet
https://www.cvedetails.com/vulnerability-list/vendor_id-3080/Fortinet.html

Fortinet delays patching zero-day allowing remote server takeover
https://www.bleepingcomputer.com/news/security/fortinet-delays-patching-zero-day-allowing-remote-server-takeover/

Fortinet fixes critical vulnerabilities in SSL VPN and web firewall
https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-vulnerabilities-in-ssl-vpn-and-web-firewall/

Fortinet FortiWeb OS Command Injection
https://www.rapid7.com/blog/post/2021/08/17/fortinet-fortiweb-os-command-injection/

Fortinet slams Rapid7 for disclosing vulnerability before end of their 90-day window
https://www.zdnet.com/article/fortinet-slams-rapid7-for-disclosing-vulnerability-before-end-of-90-day-window/