MUST READ: Ubuntu 22.04 beta has arrived and it's one of the best releases from Canonical yet

Fortinet slams Rapid7 for disclosing vulnerability before end of their 90-day window

Rapid7 disputed the idea that the 90-day window applied to them.

Written by **Jonathan Greig**,
Staff Writer

on August 17, 2021 | Topic: Security

A dispute broke out on Tuesday after cybersecurity company Rapid7 released a report (https://www.rapid7.com/blog/post/2021/08/17/fortinet-fortiweb-os-command-injection/) about a vulnerability in a Fortinet product before the company had time to release a patch addressing the issue.

Rapid7 said one of its researchers, William Vu, discovered an OS command injection vulnerability in version 6.3.11 and prior to FortiWeb's management interface. The vulnerability allows remote, authenticated attackers to execute arbitrary commands on the system through the SAML server configuration page.

Rapid7 said the vulnerability was related to CVE-2021-22123 (https://www.fortiguard.com/psirt/FG-IR-20-120), which was addressed in FG-IR-20-120. The company added that in the absence of a patch, users should "disable the FortiWeb device's management interface from untrusted networks, which would include the internet."

The report included a timeline that said Rapid7 contacted Fortinet about the vulnerability in June, and Fortinet acknowledged it by June 11. Rapid7 claims they never heard from Fortinet again until they publicly released the report on Tuesday.

A Fortinet spokesperson contacted *ZDNet* after the story on this vulnerability (https://www.zdnet.com/article/patch-released-for-fortinet-command-injection-vulnerability/) was published to

criticize Rapid7 for violating the terms of their disclosure agreement. Fortinet said it has a clear disclosure policy on its PSIRT Policy page (https://www.fortiguard.com/psirt_policy) which includes "asking incident submitters to maintain strict confidentiality until complete resolutions are available for customers."

"We had expected that Rapid7 hold any findings prior to the end of our 90-day Responsible disclosure window (https://www.fortiguard.com/zeroday/responsible-disclosure). We regret that in this instance, individual research was fully disclosed without adequate notification prior to the 90-day window," the Fortinet spokesperson said, adding that they often work closely with researchers and vendors on cybersecurity.

"We are working to deliver immediate notification of a workaround to customers and a patch released by the end of the week."

Fortinet did not respond to follow up questions about the patch for the vulnerability.

Rapid7 updated their report to say that Fortiweb 6.4.1 will be released at the end of August and will have a fix for the vulnerability.

Rapid7 disputed the idea that they had violated any part of Fortinet's rules, noting that the 90-day window Fortinet continues to mention is only their own disclosure as a vendor (https://www.fortiguard.com/zeroday/responsible-disclosure) identifying other vulnerabilities. According to Rapid7, Fortinet's own policies for organizations that may suspect vulnerabilities within Fortinet's network do not mention a 90-day window.

Rapid7 said they contacted Fortinet multiple times to work on the issue but didn't get a response, so they followed their own disclosure policies (https://www.rapid7.com/security/disclosure/#zeroday) when releasing the report.

Tod Beardsley, director of research at Rapid7, told *ZDNet* that their vulnerability disclosure policy outlines a 60-day minimum for disclosing vulnerabilities after initial contact attempts.

"In this instance, the initial disclosure was presented to Fortinet on June 10, and a vendor ticket was received on June 11, per our disclosure report. We made several follow-up attempts with Fortinet following that initial communication, and unfortunately, we received no response back after 66 days," Beardsley explained.

"There was no violation of disclosure policies. Shortly after publishing the disclosure, we were in contact with Fortinet, and they indicated they would be releasing a fix. Once that fix

is released, we'll update our disclosure with that link and CVE ID."

Beardsley added that there is no indication the vulnerability has been used, so Rapid7's disclosure "should be read as a cautionary piece for users of Fortinet's FortiWeb."

He reiterated that users of FortiWeb should not expose their management interface to the internet in general and should make sure that the people with authentication credentials are picking solid, strong passwords.

SECURITY

Using Russian tech? Look at the risks again (https://www.zdnet.com/article/using-russian-tech-its-time-to-look-at-the-risks-again-says-cybersecurity-chief/)

Hundreds more packages found in malicious npm 'factory' (https://www.zdnet.com/article/hundreds-more-malicious-packages-found-in-npm-factory/)

The 5 best VPN services compared (https://www.zdnet.com/article/best-vpn/)

Apple updates macOS, iOS, and iPadOS to fix possibly exploited zero-day flaws (https://www.zdnet.com/article/apple-updates-macos-ios-and-ipados-to-fix-possibly-exploited-zero-day-flaws/)

Is it safe to use text messages for 2-factor authentication? (https://www.zdnet.com/article/is-it-ok-to-use-text-messages-for-2-factor-authentication-ask-zdnet/)