They’ve begun: Attacks exploiting vulnerability with maximum 10 severity rating

Getty Images

reader comments

27 with

Ransomware hackers have started exploiting one or more recently fixed vulnerabilities that pose a grave threat to enterprise networks around the world, researchers said.

One of the vulnerabilities has a severity rating of 10 out of a possible 10 and another 9.9. They reside in WS_FTP Server, a file-sharing app made by Progress Software. Progress Software is the maker of MOVEit, another piece of file-transfer software that was recently hit by a critical zero-day vulnerability that has led to the compromise of more than 2,300 organizations and the data of more than 23 million people, according to security firm Emsisoft. Victims include Shell, British Airways, the US Department of Energy, and Ontario’s government birth registry, BORN Ontario, the latter of which led to the compromise of information for 3.4 million people.

About as bad as it gets

CVE-2023-40044, as the vulnerability in WS_FTP Server is tracked, and a separate vulnerability tracked as CVE-2023-42657 that was patched in the same October 27 update from Progress Software, are both about as critical as

vulnerabilities come. With a severity rating of 10, CVE-2023-40044 allows attackers to execute malicious code with high system privileges with no authentication required. CVE-2023-42657, which has a severity rating of 9.9, also allows for remote code execution but requires the hacker to first be authenticated to the vulnerable system.

Last Friday, researchers from security firm Rapid7 delivered the first indication that at least one of these vulnerabilities might be under active exploitation in "multiple instances. On Monday, the researchers updated their post to note they had discovered a separate attack chain that also appeared to target the vulnerabilities. Shortly afterward, researchers from Huntress confirmed an "in-the-wild exploitation of CVE-2023-40044 in a very small number of cases within our partner base (single digits currently)." In an update Tuesday, Huntress said that on at least one hacked host, the threat actor added persistence mechanisms, meaning it was attempting to establish a permanent presence on the server.

Advertisement

Also on Tuesday came a post on Mastodon from Kevin Beaumont, a security researcher with extensive ties to organizations whose enterprise networks are under attack.

"An org hit by ransomware is telling me the threat actor got in via WS_FTP, for infos, so you might want to prioritize patching that," he wrote. "The ransomware group targeting WS_FTP are targeting the web version." He added advice for admins using the file transfer program to search for vulnerable entry points using the Shodan search tool.

A bit shocking

On the same day that Rapid7 first saw active exploits, someone published proof of concept exploit code on social media. In an emailed statement, Progress Software officials criticized such

actions. They wrote:

> *We are disappointed in how quickly third parties released a proof of concept (POC), reverse-engineered from our vulnerability disclosure and patch, released on Sept. 27. This provided threat actors a roadmap on how to exploit the vulnerabilities while many of our customers were still in the process of applying the patch. We are not aware of any evidence that these vulnerabilities were being exploited prior to that release. Unfortunately, by building and releasing a POC rapidly after our patch was released, a third-party has given cyber criminals a tool to attempt attacks against our customers. We are encouraging all WS_FTP server customers to patch their environments as quickly as possible.*

CVE-2023-40044 is what's known as a deserialization vulnerability, a form of bug in code that allows user-submitted input to be converted into a structure of data known as an object. In programming, objects are variables, functions, or data structures that an app refers to. By essentially transforming untrusted user input into code of the attacker's making, deserialization exploits have the potential to carry severe consequences. The deserialization vulnerability in WS_FTP Server is found in code written in the .NET programming language.

Advertisement

Researchers from security firm Assetnote discovered the vulnerability by decompiling and analyzing the WS_FTP Server code. They eventually identified a "sink," which is code designed to receive incoming events, that was vulnerable to deserialization and worked their way back to the source.

"Ultimately, we discovered that the vulnerability could be triggered without any authentication, and it affected the entire Ad Hoc Transfer component of WS_FTP," Assetnote

researchers wrote Monday. “It was a bit shocking that we were able to reach the deserialization sink without any authentication.”

Besides requiring no authentication, the vulnerability can be exploited by sending a single HTTP request to a server, as long as there’s what’s known as a ysoserial gadget pre-existing.

The WS_FTP Server vulnerability may not pose as grave a threat to the Internet as a whole compared to the exploited vulnerability in MOVEit. One reason is that a fix for WS_FTP Server became publicly available before exploits began. That gave organizations using the file-transfer software time to patch their servers before they came under fire. Another reason: Internet scans find many fewer servers running WS_FTP Server as compared to MOVEit.

Still, the damage to networks that have yet to patch CVE-2023-40044 will likely be as severe as what was inflicted on unpatched MOVEit servers. Admins should prioritize patching, and if that’s not possible right away, disable server-ad hoc transfer mode. They should also analyze their environments for signs they’ve been hacked. Indicators of compromise include:

- 103[.]163[.]187[.]12:8080
- 64[.]227[.]126[.]135
- 86[.]48[.]3[.]172
- 103[.]163[.]187[.]12
- 161[.]35[.]27[.]144
- 162[.]243[.]161[.]105
- C:\Windows\TEMP\zpvmRqTOsP.exe
- C:\Windows\TEMP\ZzPtgYwodVf.exe

Other helpful security guidance is available here from security firm Tenable.

https://arstechnica.com/?p=1973010