Hackers are exploiting a flaw in Citrix software despite fix

November 20 2023, by Katrina Manson, Bloomberg News

Credit: CC0 Public Domain

A critical flaw in software from Citrix Systems Inc., a company that pioneered remote access so people can work anywhere, has been exploited by government-backed hackers and criminal groups, according to a U.S. cyber official.

The flaw, dubbed Citrix Bleed, was abused by hackers in secret for

weeks before it was found and a fix was issued last month, according to Citrix online posts and cybersecurity researchers. Since then, researchers say hackers have accelerated their exploitation of the bug, targeting some of the thousands of customers that haven't applied a patch.

"We are aware that a wide variety of malicious actors, including both nation state and criminal groups, are focused on leveraging the Citrix Bleed vulnerability," Eric Goldstein, executive assistant director for cybersecurity at the US Cybersecurity and Infrastructure Security Agency, known as CISA, told Bloomberg News.

CISA is providing assistance to victims, said Goldstein, who declined to identify them. Adversaries could exploit the vulnerability to steal sensitive information and attempt to gain broader network access, he said.

Citrix didn't respond to messages seeking comment.

Among the criminal groups exploiting the Citrix Bleed bug is one of the world's most notorious hacking gangs, LockBit, according to a global banking security consortium, the FS-ISAC, which on Tuesday issued a security bulletin about the risk to financial institutions.

The US Treasury has also said it's investigating whether Citrix vulnerabilities are responsible for the recent debilitating ransom hack against the Industrial & Commercial Bank of China Ltd., according to a person familiar with the matter. The breach rendered the world's largest bank unable to clear swaths of US Treasury trades. ICBC didn't respond to a request for comment.

LockBit claimed credit for the ICBC hack, and a representative for the gang said the bank paid a ransom, though Bloomberg wasn't able to independently confirm the claim. The Wall Street Journal previously

reported the U.S. Treasury note.

Citrix announced it had discovered the Citrix Bleed bug on Oct. 10 and issued a patch. The company said that at the time, there was no sign anyone had exploited the vulnerability.

Since then, however, multiple Citrix customers have discovered that they were breached before the patch was issued, according to a Citrix post and cybersecurity researchers. One early victim was a European government, according to a person familiar with the matter, who declined to name the country.

The Citrix Bleed bug can allow a hacker to take control of a victim's system, according to CISA. The flaw earned its nickname because it can leak sensitive information from a device's memory, according to Palo Alto Networks Inc.'s cybersecurity company research arm, Unit 42. The leaked data can include "session tokens" that can identify and authenticate a visitor to a specific website or service without entering a password.

The cybersecurity firm Mandiant started looking into the vulnerability once Citrix had flagged it and ultimately found multiple victims from before the bug had been made public or had a fix, dating back to late August.

Charles Carmakal, chief technology officer at Mandiant's consulting arm, told Bloomberg that those initial attacks didn't appear financially motivated. Mandiant is still assessing whether those early intrusions were conducted for espionage purposes by a nation state, possibly China, he said.

Asked for comment, the Chinese embassy in Washington didn't address the Citrix vulnerability but instead referred to Nov. 10 comments from

the Ministry of Foreign Affairs. "ICBC is closely following this and has taken effective emergency response measures and engaged in proper supervision and communication in order to minimize risk, impact and damage," the ministry said.

Citrix updated its guidance on Oct. 23 recommending not only patching but "killing all active and persistent sessions."

Thousands of companies failed to update their Citrix software and take other actions that the company, CISA and others have urgently recommended. Palo Alto's Unit 42 teams, which have also observed ransomware groups exploiting the bug, said in a Nov. 1 blog that at least 6,000 IP addresses appeared vulnerable and that the largest number of these devices are located in the US, as well as others in Germany, China and the UK.

GreyNoise, a company that analyzes scanning by IP addresses, reported that it's seen 335 unique IP addresses attempting to use the Citrix Bleed exploit since it started tracking it on Oct. 17.

LockBit is both the name of a gang and a type of ransomware it produced. The FBI says it is responsible for more than 1,700 attacks against the US since 2020.

A security researcher, Kevin Beaumont, said LockBit's exploitation of the Citrix flaw extends to multiple victims. The law firm Allen & Overy was breached via the Citrix flaw, he said in a post on Medium, and the aviation giant Boeing Co. and port operator DP World Plc had unpatched Citrix devices, allowing hackers to potentially exploit the bug.

Beaumont described the flaw as "incredibly easy to exploit" and added, "The cybersecurity reality we live in now is teenagers are running around in organized crime gangs with digital bazookas."

Representatives for Allen & Overy, DP World and Boeing didn't address whether the Citrix bug was exploited. The incident at Allen & Overy impacted a small number of storage servers but core systems have not been affected, a spokesperson said. The breach affecting Boeing's parts and distribution system remains under investigation, a spokesperson said.

A representative for DP World said the company is limited in the details it could provide due to the ongoing nature of the investigation. Beaumont didn't respond to a request for comment.