

Health info for 1 million patients stolen using critical GoAnywhere vulnerability

Getty Images

reader comments

28 with

Share this story

One of the biggest hospital chains in the US said hackers obtained protected health information for 1 million patients after exploiting a vulnerability in an enterprise software product called GoAnywhere.

Community Health Systems of Franklin, Tennessee, said in a filing with the Securities and Exchange Commission on Monday that the attack targeted GoAnywhere MFT, a managed file transfer product Fortra licenses to large organizations. The filing said that an ongoing investigation has so far revealed that the hack likely affected 1 million individuals. The compromised data included protected health information as defined by the Health Insurance Portability and Accountability Act, as well as patients' personal information.

Two weeks ago, journalist Brian Krebs said on Mastodon that cybersecurity firm Fortra had issued a private advisory to customers warning that the company had recently learned of a "zero-day remote code injection exploit" targeting GoAnywhere.

The vulnerability has since gained the designation CVE-2023-0669. Fortra patched the vulnerability on February 7 with the release of 7.1.2.

“The attack vector of this exploit requires access to the administrative console of the application, which in most cases is accessible only from within a private company network, through VPN, or by allow-listed IP addresses (when running in cloud environments, such as Azure or AWS),” the advisory quoted by Krebs said. It went on to say hacks were possible “if your administrative interface had been publicly exposed and/or appropriate access controls cannot be applied to this interface.”

Despite Fortra saying attacks were, in most cases, possible only on a customer’s private network, the Community Health Systems filing said Fortra was the entity that “had experienced a security incident” and learned of the “Fortra breach” directly from the company.

“As a result of the security breach experienced by Fortra, Protected Health Information (“PHI”) (as defined by the Health Insurance Portability and Accountability Act (“HIPAA”)) and “Personal Information” (“PI”) of certain patients of the Company’s affiliates were exposed by Fortra’s attacker,” the filing stated.

Advertisement

In an email seeking clarification on precisely which company’s network was breached, Fortra officials wrote: “On January 30, 2023, we were made aware of suspicious activity within certain instances of our GoAnywhere MFTaaS solution. We immediately took multiple steps to address this, including implementing a temporary outage of this service to prevent any further unauthorized activity, notifying all customers who may have been impacted, and sharing mitigation guidance, which includes instructions to our on-prem customers about applying our recently developed patch.” The statement didn’t elaborate.

Fortra declined to comment beyond what was published in Monday's SEC filing.

Last week, security firm Huntress reported that a breach experienced by one of its customers was the result of an exploit of a GoAnywhere vulnerability that most likely was CVE-2023-0669. The breach occurred on February 2 at roughly the same time Krebs had posted the private advisory to Mastodon.

Huntress said that the malware used in the attack was an updated version of a family known as Truebot, which is used by a threat group known as Silence. Silence, in turn, has ties to a group tracked as TA505, and TA505 has ties to a ransomware group, Clap.

"Based on observed actions and previous reporting, we can conclude with moderate confidence that the activity Huntress observed was intended to deploy ransomware, with potentially additional opportunistic exploitation of GoAnywhere MFT taking place for the same purpose," Huntress researcher Joe Slowick wrote.

More evidence Clap is responsible came from Bleeping Computer. Last week, the publication said Clap members took responsibility for using CVE-2023-0669 to hack 130 organizations but provided no evidence to support the claim.

In an analysis, researchers with security company Rapid7 described the vulnerability as a "pre-authentication deserialization issue" with "very high" ratings for exploitability and attacker value. To exploit the vulnerability, attackers need either network-level access to GoAnywhere MFT's administration port (by default, port 8000) or the ability to target an internal user's browser.

Given the ease of attacks and the effective release of proof-of-concept code that exploits the critical vulnerability, organizations that use GoAnywhere should take the threat

seriously. Patching is, of course, the most effective way of preventing attacks. Stop-gap measures GoAnywhere users can take in the event they can't patch immediately are to ensure that network-level access to the administrator port is restricted to the least number of users possible and to remove browser users' access to the vulnerable endpoint in their web.xml file.

<https://arstechnica.com/?p=1917988>