

GoAnywhere MFT Users Warned of Zero-Day Exploit

Users of the GoAnywhere secure managed file transfer (MFT) software have been warned about a zero-day exploit that malicious actors can target directly from the internet.

The GoAnywhere MFT is made by Fortra, known until recently as HelpSystems, and it's designed to enable organizations to automate and secure the exchange of data with their trading partners.

Cybersecurity blogger Brian Krebs broke the news about the zero-day vulnerability on Thursday, saying that the company had temporarily implemented a service outage in response.

An advisory obtained by Krebs – it can only be accessed by authenticated users – describes it as a zero-day remote code injection exploit and says that “the attack vector of this exploit requires access to the administrative console of the application”.

According to the vendor, the vulnerable admin console should in most cases only be accessible from within a company's network, through a VPN, or only by trusted IP addresses. However, the company has admitted that some GoAnywhere users may be exposing the console to the public internet.

Fortra noted that the web client interface, which is typically accessible from the internet, is not affected by the exploit.

The advisory doesn't clearly say that the vulnerability has been exploited in the wild, but active exploitation is likely, considering that it has been described as a zero-day. In addition, the vendor provides instructions on how customers can check if their system has been compromised.

The best indicator of compromise (IoC), according to the advisory, is the presence of suspicious administrator accounts that may have been created by malicious actors.

The advisory does not mention a patch, but it does recommend mitigations that should prevent exploitation. There is also no mention of a CVE identifier for the vulnerability in the advisory obtained by Krebs.

Security researcher Kevin Beaumont has conducted a Shodan search and found roughly 1,000 internet-exposed systems, a majority located in the United States. However, some of the results are clearly labeled as being associated with the web client, which Fotra says is not impacted.

Related: Zero-Day Vulnerability Exploited to Hack Over 1,000 Zimbra Email Servers

Related: US Agencies Warn of APTs Exploiting Recent ADSelfService Plus Zero-Day

Related: Accellion Failed to Notify Customers of FTA Zero-Day

<https://www.securityweek.com/goanywhere-mft-users-warned-of-zero-day-vulnerability/>

ro-day-exploit/