Procter & Gamble confirms data theft via GoAnywhere zero-day

By Sergiu Gatlan

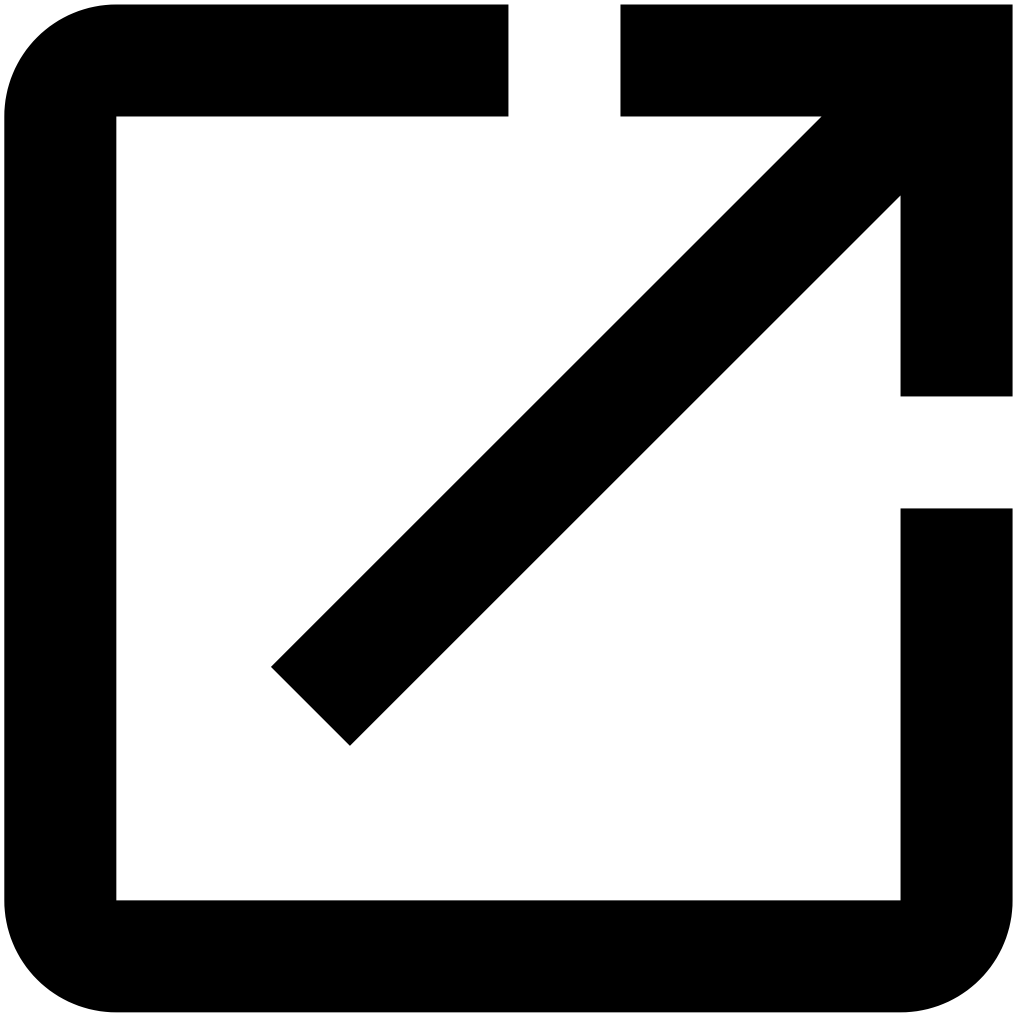
Published: 2023-03-24 · Archived: 2026-04-05 12:54:08 UTC

Consumer goods giant Procter & Gamble has confirmed a data breach affecting an undisclosed number of employees after its GoAnywhere MFT secure file-sharing platform was compromised in early February.

While the company didn't say who was behind the security breach, this is part of an ongoing spree of extortion demands linked to the Clop ransomware gang's attacks targeting Fortra GoAnywhere secure storage servers worldwide.

According to Procter & Gamble, the attackers didn't gain access to employees' financial or social security information, although they did manage to steal some of their data.


DIE LINKE.
0:00



"P&G can confirm that it was one of the many companies affected by Fortra's GoAnywhere incident. As part of this incident, an unauthorized third party obtained some information about P&G employees," Procter & Gamble told BleepingComputer.

"The data that was obtained by the unauthorized party did not include information such as Social Security numbers or national identification numbers, credit card details, or bank account information."

P&G says it has no evidence that this data breach impacted customer data and that it stopped using Fortra's GoAnywhere secure file-sharing services after discovering the incident.

"When we learned of this incident in early February, we promptly investigated the nature and scope of the issue, disabled [the] use of the vendor's services, and notified employees," the company added.

"At this time, there is no indication that customer data was affected by this issue. Our business operations are continuing as normal."

Clop claims it stole files from over 130 organizations

The Clop ransomware gang previously told Bleeping Computer that it exploited the CVE-2023-0669 GoAnywhere vulnerability as a zero-day to breach and steal data from the secure storage servers of more than 130 organizations.

They allegedly stole the data over ten days after breaching Internet-exposed servers vulnerable to exploits targeting this bug.

The threat actors also claimed they only stole the documents stored on the victims' compromised file-sharing platforms, although they could've also easily moved laterally through their networks to deploy ransomware payloads.

Clop began publicly extorting the GoAnywhere attacks' victims on March 10 when it added seven companies to its data leak site.

So far, the list of victims who came forward to acknowledge GoAnywhere breaches and that Clop is extorting them also includes healthcare giant Community Health Systems (CHS), fintech platform Hatch Bank, cybersecurity firm Rubrik, Hitachi Energy, luxury brand retailer Saks Fifth Avenue, and the City of Toronto, Canada.

In ransom notes sent to the victims and seen by BleepingComputer, the ransomware gang introduces themselves as the "Clop hacker group," warning victims that they'd stolen sensitive documents, which would be published online on Clop's leak site and sold on the black market if the victims were unwilling to negotiate.

"We want to inform you that we have stolen important information from your GoAnywhere MFT resource and have attached a full list of files as evidence," the ransom notes read.

"We deliberately did not disclose your organization and wanted to negotiate with you and your leadership first. If you ignore us, we will sell your information on the black market and publish it on our blog, which receives 30-50 thousand unique visitors per day."

Also behind the 2020 Accellion breaches

The ransomware gang's alleged use of a GoAnywhere MFT zero-day to steal sensitive files from victims' secure sharing servers is very similar to using an Accellion FTA zero-day vulnerability to steal the data of roughly 100 companies in December 2020.

In the Accellion attacks, Clop stole massive amounts of data and demanded $10 million ransoms from high-profile companies such as energy giant Shell, cybersecurity firm Qualys, supermarket giant Kroger, and universities worldwide (e.g., Stanford Medicine, University of Colorado, and the University of California).

The Clop gang has also been linked to ransomware attacks since at least 2019, encrypting and stealing files from the servers of a long string of victims, including Software AG IT, Maastricht University, ExecuPharm, and Indiabulls.

Source: https://www.bleepingcomputer.com/news/security/procter-and-gamble-confirms-data-theft-via-goanywhere-zero-day/