

GoAnywhere Zero-Day Attack Hits Major Orgs

More organizations are emerging to confirm impact from the newly disclosed in-the-wild zero-day exploits hitting Fortra's GoAnywhere managed file transfer (MFT) software.

Tracked as CVE-2023-0669, the vulnerability was publicly disclosed in early February alongside zero-day exploitation and a patch was released a week later.

Soon after, attacks targeting the security defect were linked to a Russian-speaking threat actor called 'Silence' that has been linked to the distribution of the Cl0p ransomware.

Over the past week, the ransomware group started posting on their Tor-based leak site the names of organizations allegedly impacted by the incident, including the City of Toronto, luxury brand retailer Saks Fifth Avenue, American education platform Pluralsight, consumer goods giant Procter & Gamble, mining company Rio Tinto, and the U.K.'s Pension Protection Fund (PPF).

Previously, sustainable energy giant Hitachi Energy, California-based digital bank Hatch Bank, cybersecurity firm Rubrik, and healthcare provider Community Health Systems confirmed impact from the GoAnywhere attack.

Responding to a *SecurityWeek* inquiry, the City of Toronto confirmed that some data was compromised in an incident at a third-party vendor, without specifically naming Fortra's GoAnywhere service.

"The access is limited to files that were unable to be processed through the third-party secure file transfer system.

The City is actively investigating the details of the identified files,” a City of Toronto official said.

Saks Fifth Avenue confirmed that some of its data was stolen following the GoAnywhere incident but claimed that no real customer data was impacted.

“Fortra, a vendor to Saks and many other companies, recently experienced a data security incident that led to mock customer data being taken from a storage location used by Saks. The mock customer data does not include real customer or payment card information and is solely used to simulate customer orders for testing purposes,” Saks told *SecurityWeek*.

Pluralsight says that it immediately discontinued the use of GoAnywhere after Fortra informed them of the incident, and that it also notified all affected customers of the risks associated with the attack.

In a statement on its website, PPF says that employee data was compromised in the GoAnywhere incident, and that it stopped using the service immediately after learning that.

P&G has confirmed that some employee data was stolen in the incident, but said the incident did not impact customer data, Social Security numbers or financial information.

Virgin confirmed not only the impact from the incident, but also that the Cl0p gang contacted them directly to claim possession of stolen data. “We were recently contacted by a ransomware group, calling themselves Cl0p, who illegally obtained some Virgin Red files via a cyber-attack on our supplier, GoAnywhere. The files in question pose no risk to customers or employees as they contain no personal data,” a Virgin Red spokesperson told *SecurityWeek*.

French digital transformation and hybrid cloud company Atos on Friday announced that the GoAnywhere incident impacted data associated with a specific Nimbix file transfer application.

“Our cybersecurity team has identified a backup folder from 2016 that was presumably exposed, due to a zero-day vulnerability known to be exploited by Cl0p. We are in contact with the clients concerned,” the company said.

According to Reuters, Rio Tinto informed employees last week that internal data, such as payroll information, was stolen in the GoAnywhere attack, and that the group responsible for the hack was threatening to release the data publicly. Rio Tinto did not respond to a *SecurityWeek* request for comment.

Related: NBA Notifying Individuals of Data Breach at Mailing Services Provider

Related: Latitude Financial Services Data Breach Impacts 300,000 Customers

Related: Data Breach at Independent Living Systems Impacts 4 Million Individuals

GoAnywhere Zero-Day Attack Hits Major Orgs