Citrix sued over Xfinity breach that exposed 36 million users' data

December 21 2023, by Ron Hurtibise, South Florida Sun Sentinel

Credit: Pixabay/CC0 Public Domain

Just three days after Xfinity disclosed that 36 million of its users' personal information was exposed in a data breach, Fort Lauderdale-based Citrix Systems Inc. is facing a class-action lawsuit accusing the firm of failing to prevent the breach.

The extent of the breach was disclosed on Monday in a notice to the Maine Attorney General by Comcast Cable Communications, which does business as Xfinity.

That day, Comcast released a notice to customers disclosing that "unauthorized access to its internal systems" had occurred between Oct. 16 and Oct. 19. Following a review, Comcast concluded on Dec. 6 that the breach exposed customer information such as usernames and passwords that the company had disguised for security purposes.

Hackers also stole some users' names, contact information, last four digits of Social Security numbers, dates of birth and/or secret questions and answers, Comcast said.

Customers logging onto their Xfinity accounts have been required to change their passwords to protect their accounts. They also are urged to set up two-factor, or multi-factor, authentication and to change passwords for other accounts that share the same username and password or security question.

By Wednesday, Citrix—which services Xfinity's website—was named as defendant in a proposed class-action lawsuit about the breach.

A Citrix spokesman, reached by email, said the company is aware of the lawsuit but said the company does not comment on pending litigation. Comcast, which was not named as a defendant in the lawsuit, did not respond to a request for information about the breach.

The suit accuses Citrix of failing to protect "highly sensitive information " in their custody that it "knew and understood" is "valuable and highly sought after by criminal parties who seek to illegally monetize" it by posting it for sale on the dark web.

The suit states that Citrix on Oct. 10 announced the vulnerability of a software product used by Xfinity and thousands of other companies known as "Citrix Bleed."

Citrix said it released a patch to fix the vulnerability at that time and issued additional mitigation guidance on Oct. 23, the lawsuit claims.

While Comcast said it "promptly patched and mitigated its systems," it said it later discovered that prior to the repair operation, between Oct. 16 and Oct. 19, "there was unauthorized access to some of (its) internal systems that (it) concluded was a result of this vulnerability," according to the lawsuit.

In a notification to the Office of the Maine Attorney General on Monday, Comcast revealed that the personal identifiable information of 35,879,455 individuals was believed to have been exposed in the breach.

The lawsuit names Jacksonville resident Francis Kirkpatrick as lead plaintiff. It was filed by the Fort Lauderdale law firm Kopelowitz Ostrow Ferguson Weiselberg Gilbert and the Tampa-based law firm The Consumer Protection Firm PLLC.

It says that Kirkpatrick has experienced "suspicious spam" after the breach that he believes to be an attempt to secure additional personal information.

The suit claims that class members have suffered from invasion of their privacy, lost or diminished value of their personal identifiable information, lost time and opportunity costs associated with attempting to mitigate consequences of the breach, and the "continued and certainly increased risk" to their information.

It seeks unspecified "compensatory and consequential damages" from

Citrix.

The website ClassAction.org, which describes itself as a group of online professionals with relationships with class action and mass tort attorneys, on Tuesday posted notice of an investigation that it said could lead to a class action lawsuit against Comcast. A news release on Tuesday by New Jersey-based Console & Associates, P.C. urges victims to contact the law firm.

According to GovTech.com, a website that serves the government technology industry, hackers have been exploiting "Citrix Bleed" vulnerabilities since August. Hackers can exploit the vulnerability within Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances, the site reported.

The vulnerability enables hackers "to bypass password requirements and multifactor authentication" to hijack "legitimate user sessions," according to an advisory released on Nov. 21 by the Cybersecurity & Infrastructure Security Agency, a component of the United States Department of Homeland Security.

"Through the takeover of legitimate user sessions, malicious actors acquire elevated permissions to harvest credentials, move laterally, and access data and resources," the advisory states.

Citrix Bleed has been linked to ransomware and malware attacks on several companies, including Toyota and Boeing, several tech sites reported.

For Comcast, news of the breach comes a year after a different breach left an unknown number of customers unable to access their accounts. When they regained access, they discovered their accounts had been taken over by hackers who were able to bypass two-factor authentication

and change their passwords, then used their information to gain access to other accounts, the website SecurityBoulevard.com reported.

2023 South Florida Sun Sentinel. Distributed by Tribune Content Agency, LLC.