Millions of Xfinity customers' info, hashed passwords feared stolen in cyberattack

35M-plus Comcast user IDs accessed by intruder via Citrix Bleed

Jessica Lyons Hardcastle

Millions of Comcast Xfinity subscribers' personal data – including potentially their usernames, hashed passwords, contact details, and secret security question-answers – was likely stolen by one or more miscreants exploiting Citrix Bleed in October.

The internet, voice, and cable TV provider this week revealed it had fallen victim to the critical information disclosure bug. Citrix disclosed and patched the flaw in its NetScaler gateway appliances on October 10 before urging IT admins to apply the update and kill all active and persistent sessions using a series of commands three days later.

By the end of October, "mass exploitation" of Citrix Bleed was underway, and ransomware crews were working to abuse and monetize the security flaw. The bug can be exploited to remotely break into corporate networks, steal data, and commit other crimes.

Despite having "promptly patched and mitigated the Citrix vulnerability within its system," during a routine cybersecurity exercise on October 25, "Xfinity discovered suspicious activity," Comcast spokesperson Joel Shadle told *The Register* today.

The US cable giant "subsequently determined that between October 16 and October 19, 2023, there was unauthorized access to its internal systems that was concluded to be a result of this vulnerability," Shadle said.

In a privacy breach notification submitted to the Maine Attorney General's office on Monday, Comcast said 35.9 million people were affected by the digital break-in.

Shandle says that number doesn't necessarily mean "customers," and that "user IDs" is a better way to put it. One customer might have multiple user IDs — for other family members, vacation properties, and the like.

Regardless, it's a massive amount of people, and potentially all of Xfinity's customers. To put it in context: in 2022, Comcast provided high-speed broadband internet access to more than 32 million customers.

After discovering the intrusion, Xfinity complained to the Feds, and by November 16 "determined that information was likely acquired," it disclosed. [PDF].

As of December 6, the potentially stolen customer data includes usernames and hashed passwords, the internet provider said. Plus, "for some customers" the crooks also likely nabbed people's names, contact information, the last four digits of Social Security numbers, dates of birth, and/or secret questions and answers.

Hashed passwords, for those who don't know, are one-way encrypted passwords: you can't directly figure out someone's actual password from their hashed password, though miscreants can attempt to deduce people's passwords from the hashes. Whether those crooks are successful or not depends on the algorithm and method used by Comcast to create the hashes, and how strong the passwords were to begin with.

Meanwhile, the telco said its "data analysis is continuing."

While your humble vulture is trying really hard to be a glass-half-full kinda bird, it's hard to shake the feeling that things are gonna get worse.

Xfinity is now requiring subscribers to reset their passwords, and "strongly recommends" enabling two- or multi-factor authentication. As always, please don't reuse passwords across multiple accounts.

If you are using the same password and security question-answer combo for other services in addition to Xfinity, save yourself some potential pain down the line and change those for your other accounts, too. ®