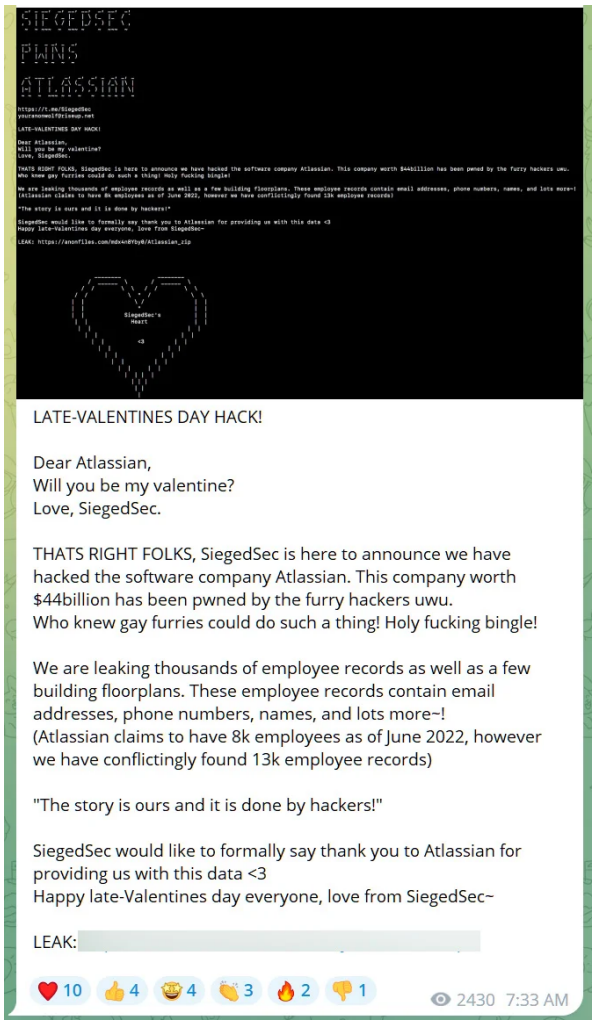
Atlassian says recent data leak stems from third-party vendor hack

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** February 16, 2023 12:41 PM **0**

Atlassian has confirmed that a breach at a third-party vendor caused a recent leak of company data and that their network and customer information is secure.

As first reported by Cyberscoop (https://cyberscoop.com/atlassian-hack-employee-data-seigedsec/), a hacking group known as SiegedSec leaked data on Telegram yesterday, claiming to be stolen from Atlassian, a collaboration software company based out of Australia.

"We are leaking thousands of employee records as well as a few building floorplans. These employee records contain email addresses, phone numbers, names, and lots more~!," said the SiegedSec hackers.



SiegedSec post on Telegram
Source: BleepingComputer

Soon after the leak, Check Point Software (https://www.checkpoint.com/) told BleepingComputer that they analyzed the leaked data and that it contained two floor maps for the Sydney and San Francisco offices and a JSON file containing information about employees.

"From the initial analysis, we suspect the group did not hack to Atlassian directly but into a 3rd party provider named https://envoy.com/," Check Point Software told BleepingComputer.

Today, Atlassian confirmed to BleepingComputer that the data breach was caused by a breach of their third-party vendor Envoy which they use for in-office functions.

"On February 15, 2023 we learned that data from Envoy, a third-party app that Atlassian uses to coordinate in-office resources, was compromised and published. Atlassian product and customer data is not accessible via the Envoy app and therefore not at risk," Atlassian told BleepingComputer.

"The safety of Atlassians is our priority, and we worked quickly to enhance physical security across our offices globally. We are actively investigating this incident and will continue to provide updates to employees as we learn more."

However, Envoy says that they are not aware of a breach on their side and believes that an Atlassian employee's credentials were stolen, allowing the threat actor access to the data inside the Envoy app.

"We're investigating this right now and are not aware of any compromise to our systems. Our initial research shows that a hacker gained access to an Atlassian employee's valid credentials to pivot and access the Atlassian employee directory and office floor plans held within Envoy's app," Envoy told BleepingComputer.

"Envoy, like Atlassian, takes the security and privacy of our customers' data incredibly seriously and has stringent measures in place to protect it."

Update 2/16/23 4:35 PM ET: Added Envoy statement

Related Articles:

JD Sports says hackers stole data of 10 million customers (https://www.bleepingcomputer.com/news/security/jd-sports-says-hackers-stole-data-of-10-million-customers/)

GoTo says hackers stole customers' backups and encryption key (https://www.bleepingcomputer.com/news/security/goto-says-hackers-stole-customers-backups-and-encryption-key/)

Restaurant CRM platform 'SevenRooms' confirms breach after data for sale (https://www.bleepingcomputer.com/news/security/restaurant-crm-platform-sevenrooms-confirms-breach-after-data-for-sale/)

Nissan North America data breach caused by vendor-exposed database (https://www.bleepingcomputer.com/news/security/nissan-north-america-data-breach-caused-by-vendor-exposed-database/)

Ransomware gang cloned victim's website to leak stolen data (https://www.bleepingcomputer.com/news/security/ransomware-gang-cloned-victim-s-website-to-leak-stolen-data/)