

# T-Mobile denies it was hacked, links leaked data to vendor breach

By [Ionut Ilascu](#)



June 19, 2024



08:43 PM



0



T-Mobile has denied it was breached or that source code was stolen after a threat actor claimed to be selling stolen data from the telecommunications company.

"T-Mobile systems have not been compromised. We are actively investigating a claim of an issue at a third-party service provider," T-Mobile shared in a statement to BleepingComputer.

"We have no indication that T-Mobile customer data or source code was included and can confirm that the bad actor's claim that T-Mobile's infrastructure was accessed is false."

This statement comes after IntelBroker, a [well-known threat actor](#) linked to [numerous breaches](#), claimed to have breached T-Mobile in June 2024 and stolen source code.

To prove that the data is authentic and originates from a recent cyberattack, IntelBroker published several screenshots showing access with administrative privileges to a Confluence server and the company's internal Slack channels for developers.

IntelBroker describes the data they're selling as "Source code, SQL files, Images, Terraform data, t-mobile.com certifications, Siloprograms."

**T-Mobile Internal Source Code Breach**  
by IntelBroker - Wednesday June 19, 2024 at 06:26 PM

20 minutes ago #1

**[Mod] IntelBroker**

Hello **BreachForums** Community  
Today, I am selling the T-Mobile Internal Data Breach.

**T-Mobile®**

Breached by @**[Mod] IntelBroker**  
In June 2024, T-Mobile's infrastructure was breached and had much of their data leaked.  
Compromised data: Source code, SQL files, Images, Terraform data, t-mobile.com certifications, Siloprograms, etc

**Samples!**  
**Tree file**

confluencesw.t-mobile.com/admin/restore-local-file.action

You have temporary access to administrative functions. Drop access if you no longer require it. For more information, refer to the documentat

T-Mobile Spaces People Calendars Blogs Analytics Create

**Confluence administration**

CONFIGURATION  
General Configuration

**Importing Data - In Progress**

**IntelBroker claiming to sell T-Mobile data from recent breach**

*source: BleepingComputer*

However, a source told BleepingComputer that the data shared by IntelBroker is actually older screenshots of T-Mobile's infrastructure posted to a third-party vendor's servers, where it was stolen.

While BleepingComputer knows the name of this alleged service provider, we will not be publicly sharing it until we can confirm if they were breached.

Recently, IntelBroker has been rapidly releasing new data breaches, and if they all used this cloud provider, it could explain where all the data is coming from.

Based on IntelBroker's screenshots, the hacker had access to a Jira instance for testing applications as recently as this month.

It is unclear how the hackers breached the provider, but one of the leaked images shows a search for critical vulnerabilities listing [CVE-2024-1597](#), which affects Confluence Data Center and Server and has a severity score of 9.8 out of 10.


Whether the third-party vendor was breached with this vulnerability is currently unknown.

BleepingComputer attempted to contact IntelBroker about this incident but was unable to make contact.



T-Mobile has dealt with multiple cybersecurity incidents in the past, this one being the third that has impacted the company in some manner in less than two years. On January 19, 2023, the telecommunications company disclosed that hackers had [stolen the personal information of 37 million customers](#).

In [May 2023](#), the mobile telco revealed that data belonging to hundreds of customers had been exposed to unknown attackers for more than a month starting in February of the same year.

[CONFLUENCE](#)[DATA BREACH](#)[JIRA](#)[T-MOBILE](#)



**IONUT ILASCU**



Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

[< PREVIOUS ARTICLE](#)

[NEXT ARTICLE >](#)