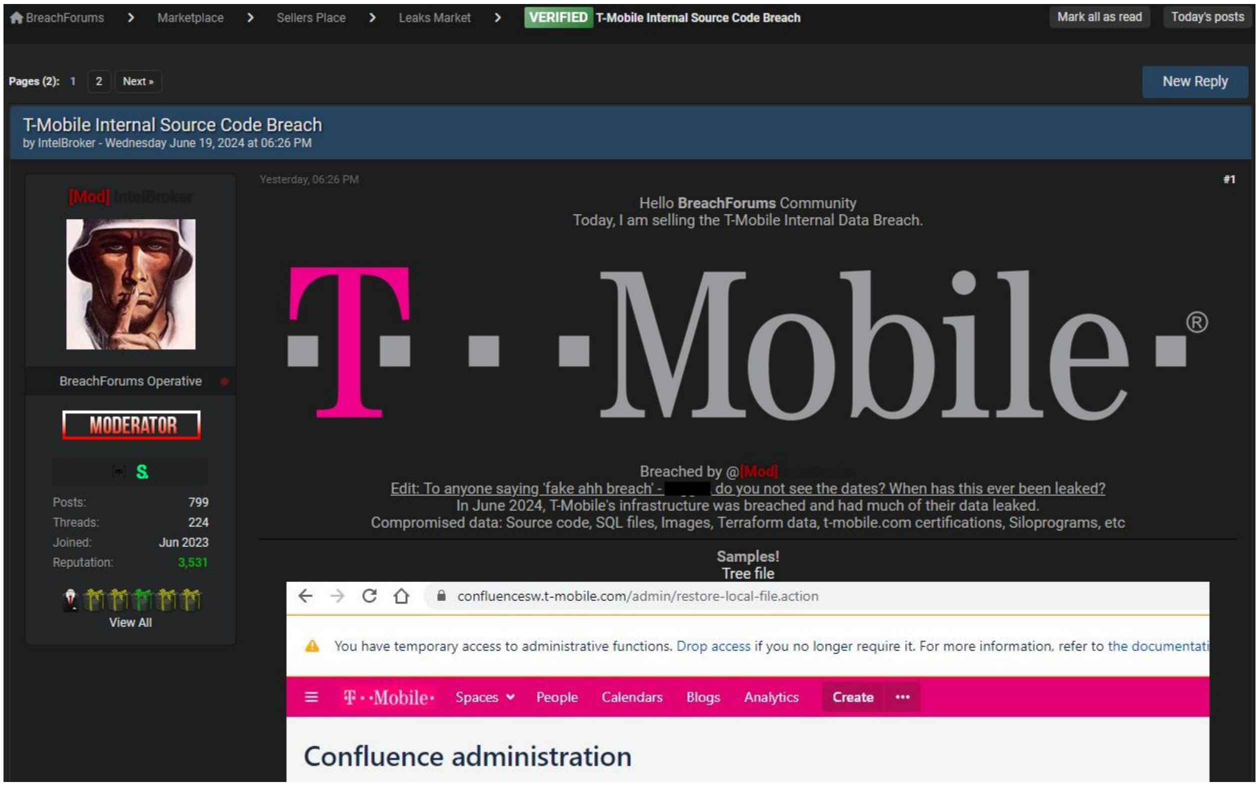
Was T-Mobile compromised by a zero-day in Jira?

malwarebytes.com/blog/news/2024/06/was-t-mobile-compromised-by-a-zero-day-in-jira

Pieter Arntz June 21, 2024

A moderator of the notorious data breach trading platform BreachForums is offering data for sale they claim comes from a data breach at T-Mobile.

The moderator, going by the name of IntelBroker, describes the data as containing source code, SQL files, images, Terraform data, t-mobile.com certifications, and “Siloprograms.” (We’ve not heard of siloprograms, and can’t find a reference to them anywhere, so perhaps it’s a mistranslation or typo.)



BreachForums > Marketplace > Sellers Place > Leaks Market > VERIFIED T-Mobile Internal Source Code Breach
Mark all as read
Today's posts
Pages (2): 1 2 Next »
New Reply

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

Posts:	799
Threads:	224
Joined:	Jun 2023
Reputation:	3,531

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

Breached by @[Mod] IntelBroker
Edit: To anyone saying 'fake ahh breach' - [redacted] do you not see the dates? When has this ever been leaked?
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 documentati

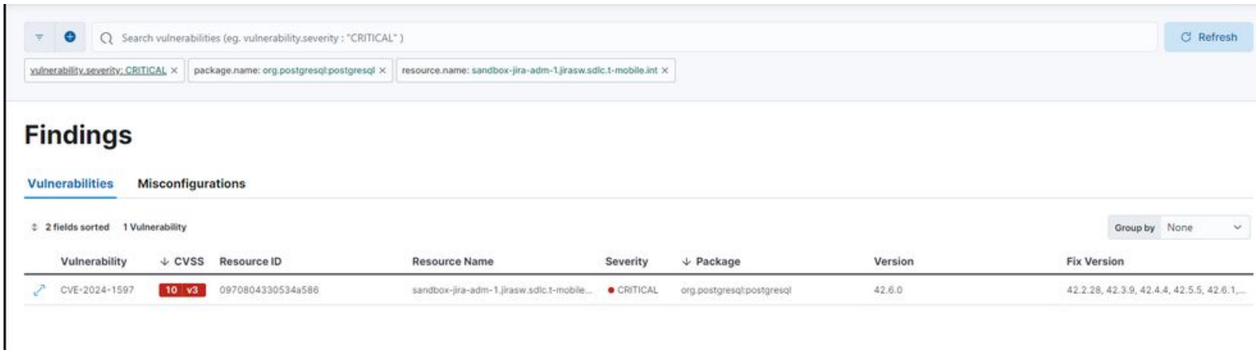
Confluence administration

Post offereing data for sale supposedly from a T-Mobile internal breach

To prove they had the data, IntelBroker posted several screenshots showing access with administrative privileges to a Confluence server and T-Mobile's internal Slack channels for developers.

But according to sources known to BleepingComputer, the data shared by IntelBroker actually consists of older screenshots. These screenshots show T-Mobile's infrastructure, posted at a known—yet unnamed—third-party vendor's servers, from where they were stolen.

When we looked at the screenshots IntelBroker attached to their post, we spotted something interesting in one of them.



Search vulnerabilities (eg. vulnerability.severity : "CRITICAL")
Refresh

vulnerability.severity: CRITICAL × package.name: org.postgresql:postgresql × resource.name: sandbox-jira-adm-1.jirasw.sdlc.t-mobile.int ×

Findings

Vulnerability	CVSS	Resource ID	Resource Name	Severity	Package	Version	Fix Version
CVE-2024-1597	10 v3	0970804330534a586	sandbox-jira-adm-1.jirasw.sdlc.t-mobile...	● CRITICAL	org.postgresql:postgresql	42.6.0	42.2.28, 42.3.9, 42.4.4, 42.5.5, 42.6.1,...

Found CVE-2024-1597

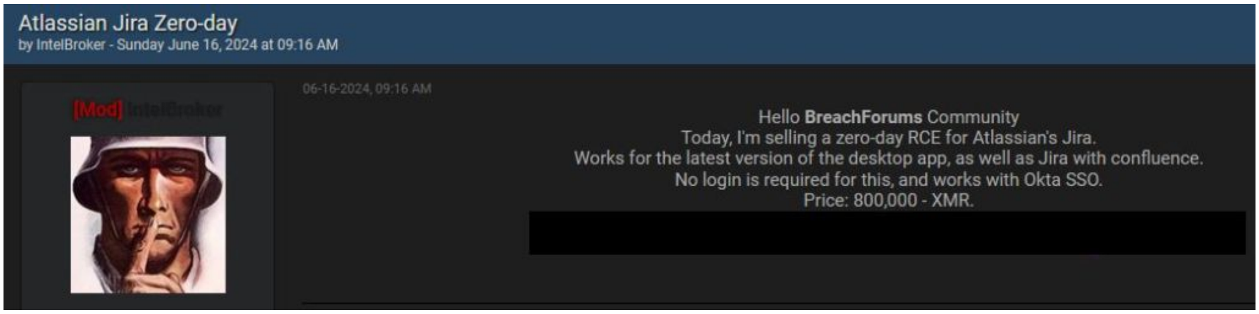
This screenshot shows a search query for a critical vulnerability in Jira, a project management tool used by teams to plan, track, release and support software. It's typically a place where you could find the source code of works in progress.

The search returns the result CVE-2024-1597, a SQL injection vulnerability. SQL injection happens when a cybercriminal injects malicious SQL code into a form on a website, such as a login page, instead of the data the form is asking for. The vulnerability affects Confluence Data Center and Server according to Atlassian's May security bulletin.

For a better understanding, it's important to note that Jira and Confluence are both products created by Atlassian, where Jira is the project management and issue tracking tool and Confluence is the collaboration and documentation tool. They are often used together.

If IntelBroker has a working exploit for the SQL injection vulnerability, this could also explain their claim that they have the source code of three internal tools used at Apple, including a single sign-on authentication system known as AppleConnect.

This theory is supported by the fact that IntelBroker is also offering a Jira zero-day for sale.



Atlassian Jira Zero-day
by IntelBroker - Sunday June 16, 2024 at 09:16 AM

[Mod] IntelBroker

06-16-2024, 09:16 AM

Hello **BreachForums** Community
Today, I'm selling a zero-day RCE for Atlassian's Jira.
Works for the latest version of the desktop app, as well as Jira with confluence.
No login is required for this, and works with Okta SSO.
Price: 800,000 - XMR.
[redacted]

IntelBroker selling zero-day for JIra

> "I'm selling a zero-day RCE for Atlassian's Jira.
>
> Works for the latest version of the desktop app, as well as Jira with confluence.
>
> No login is required for this, and works with Okta SSO."

If this is true then this exploit, or its fruits, might be used for data breaches that involve personal data.

Meanwhile, T-Mobile has denied it has suffered a breach, saying it is investigating whether there has been a breach at a third-party provider.

> "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."

We don't just report on threats – we help safeguard your entire digital identity

Cybersecurity risks should never spread beyond a headline. Protect your—and your family's—personal information by using identity protection.