Okta's source code stolen after GitHub repositories hacked

By
Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)

December 21, 2022 01:15 AM **0**

Okta, a leading provider of authentic
Management (IAM) solutions, says
this month.

According to a 'confidential' email notification sent by Okta and seen by BleepingComputer, the security incident involves threat actors stealing Okta's source code.

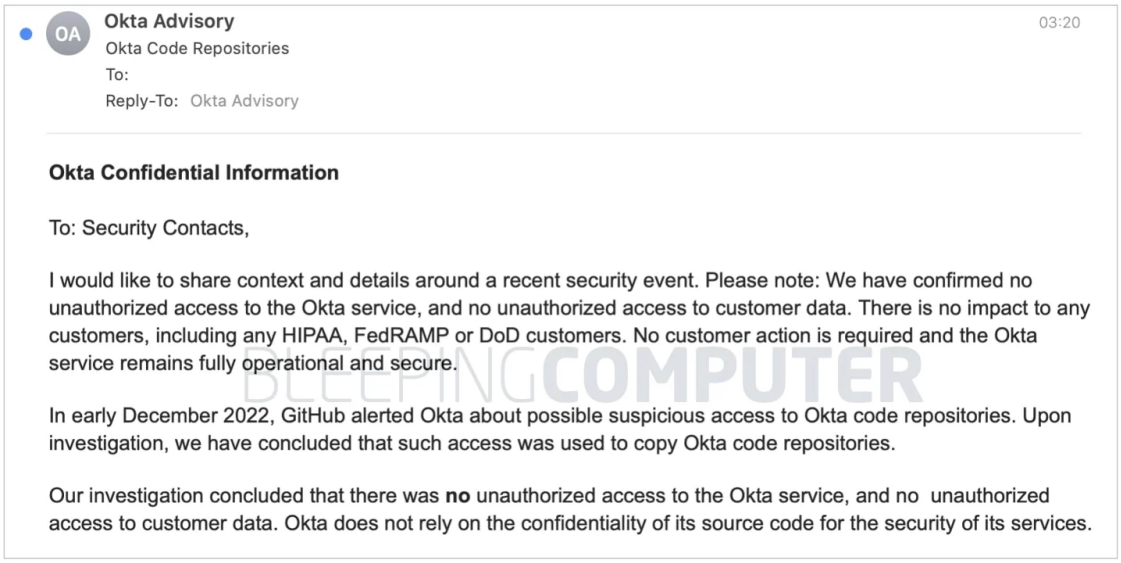
Source code stolen, customer data not impacted

BleepingComputer has obtained a 'confidential' security incident notification that Okta has been emailing to its 'security contacts' as of a few hours ago. We have confirmed that multiple sources, including IT admins, have been receiving this email notification.

Earlier this month, GitHub alerted Okta of suspicious access to Okta's code repositories, states the notification.

"Upon investigation, we have concluded that such access was used to copy Okta code repositories," writes David Bradbury, the company's Chief Security Officer (CSO) in the email.

Despite stealing Okta's source code, attackers did not gain unauthorized access to the Okta service or customer data, says the company. Okta's "HIPAA, FedRAMP or DoD customers" remain unaffected as the company "does not rely on the confidentiality of its source code as a means to secure its services." As such, no customer action is needed.



Okta Advisory
Okta Code Repositories
To:
Reply-To: Okta Advisory
03:20

Okta Confidential Information

To: Security Contacts,

I would like to share context and details around a recent security event. Please note: We have confirmed no unauthorized access to the Okta service, and no unauthorized access to customer data. There is no impact to any customers, including any HIPAA, FedRAMP or DoD customers. No customer action is required and the Okta service remains fully operational and secure.

In early December 2022, GitHub alerted Okta about possible suspicious access to Okta code repositories. Upon investigation, we have concluded that such access was used to copy Okta code repositories.

Our investigation concluded that there was **no** unauthorized access to the Okta service, and no unauthorized access to customer data. Okta does not rely on the confidentiality of its source code for the security of its services.

Okta emails its 'security contacts' a security notification (BleepingComputer)

At the time of writing our report, the incident appears to be relevant to Okta Workforce Identity Cloud (WIC) code repositories, but not Auth0 Customer Identity Cloud product, given the email wording.

An excerpt from the remainder of the notification, reviewed by BleepingComputer, is published below:

> As soon as Okta learned of the possible suspicious access, we promptly placed temporary restrictions on access to Okta GitHub repositories and suspended all GitHub integrations with third-party applications.
>
> We have since reviewed all recent access to Okta software repositories hosted by GitHub to understand the scope of the exposure, reviewed all recent commits to Okta software repositories hosted with GitHub to validate the integrity of our code, and rotated GitHub credentials. We have also notified law enforcement.
>
> Additionally, we have taken steps to ensure that this code cannot be used to access company or customer environments. Okta does not anticipate any disruption to our business or our ability to service our customers as a result of this event.
>
> Note: The security event pertains to Okta Workforce Identity Cloud (WIC) code repositories. It does not pertain to any Auth0 (Customer Identity Cloud) products.
>
> We have decided to share this information consistent with our commitment to transparency and partnership with our customers.

While ending its 'confidential' email that pledges a 'commitment to transparency,' Okta says it will publish a statement today on its blog.

BleepingComputer reached out to O
reply was not immediately available

Okta security incidents: year in review

It's been a difficult year for Okta with its series of security incidents and bumpy disclosures.

September this year, Okta-owned Auth0 disclosed a similar-style incident (https://www.bleepingcomputer.com/news/security/auth0-warns-that-some-source-code-repos-may-have-been-stolen/). According to the authentication service provider, older Auth0 source code repositories were obtained by a "third-party individual" from its environment via unknown means. But, Okta's problems began long before, amid the irregularity surrounding the disclosure of its January hack.

March this year, data extortion group Lapsus$ claimed it had access to Okta's (https://www.bleepingcomputer.com/news/security/okta-investigating-claims-of-customer-data-breach-from-lapsus-group/) administrative consoles and customer data as it began posting screenshots of the stolen data on Telegram.

After stating that it was investigating these claims, Okta shortly acknowledged that the hack being referred to had in fact occurred late January 2022 and potentially affected 2.5% of its customers (https://www.bleepingcomputer.com/news/security/okta-confirms-25-percent-customers-impacted-by-hack-in-january/). This figure was estimated to be roughly 375 organizations at the time, given Okta's 15,000+ customer base back then (https://web.archive.org/web/20220314190142/https://www.okta.com/company/).

The same week, Okta admitted that it had "made a mistake" in delaying the disclosure (https://www.bleepingcomputer.com/news/security/okta-we-made-a-mistake-delaying-the-lapsus-hack-disclosure/) of this hack that, the firm said, had originated at its third-party contractor, Sitel (Sykes).

In April, Okta clarified that the January breach had lasted "25 consecutive minutes" and the impact was significantly smaller than what was originally anticipated: limited to just two customers (https://www.bleepingcomputer.com/news/security/okta-lapsus-breach-lasted-only-25-minutes-hit-2-customers/).

Related Articles:

GitHub to require all users to enable 2FA by the end of 2023 (https://www.bleepingcomputer.com/news/security/github-to-require-all-users-to-enable-2fa-by-the-end-of-2023/)

GitHub rolls out free secret scanning for all public repositories (https://www.bleepingcomputer.com/news/security/github-rolls-out-free-secret-scanning-for-all-public-repositories/)

Okta shares fix for issue impacting Microsoft 365 SSO logins (https://www.bleepingcomputer.com/news/technology/okta-shares-fix-for-issue-impacting-microsoft-365-sso-logins/)

Microsoft sued for open-source piracy through GitHub Copilot (https://www.bleepingcomputer.com/news/security/microsoft-sued-for-open-source-piracy-through-github-copilot/)

Dropbox discloses breach after hacker stole 130 GitHub repositories (https://www.bleepingcomputer.com/news/security/dropbox-discloses-breach-after-hacker-stole-130-github-repositories/)

GITHUB (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/GITHUB/)

OKTA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/OKTA/)

SOURCE CODE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SOURCE-CODE/)

THEFT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/THEFT/)

(https://www.bleepingcomputer.com/author/ax-sharma/)

AX SHARMA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/AX-SHARMA/)

(MAILTO:AX@AXSHARMA.COM) (HTTPS://TWITTER.COM/AX_SHARMA)

Ax Sharma is a Security Researcher and Tech Reporter. His works and expert analyses have frequently been featured by leading media outlets including the BBC, Business Insider, Fortune, TechCrunch, The Register, and others. Ax's expertise lies in vulnerability research, malware analysis, and open source software. He's an active community member of British Association of Journalists (BAJ) and Canadian Association of Journalists (CAJ). Send any tips via email or Twitter DM.

PREVIOUS ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/MICROSOFT-PUSHES-EMERGENCY-FIX-FOR-WINDOWS-SERVER-HYPER-V-VM-ISSUES/)

NEXT ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/GODFATHER-ANDROID-MALWARE-TARGETS-400-BANKS-CRYPTO-EXCHANGES/)

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now
(https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

You may also like:

POPULAR STORIES

Microsoft: KB5021233 causes blue screens with 0xc000021a errors

(https://www.bleepingcomputer.com/news/microsoft/microsoft-kb5021233-causes-blue-screens-with-0xc000021a-errors/)

Microsoft finds macOS bug that lets malware bypass security checks

(https://www.bleepingcomputer.com/news/security/microsoft-finds-macos-bug-that-lets-malware-bypass-security-checks/)

FOLLOW US:

(https://twitter.com/BleepingComputer) (https://www.facebook.com/BleepingComputer) (https://www.youtube.com/user/BleepingComputer) (https://www.bleepingcomputer.com/feed/)

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomp

Uninstall Database (https://www.bleepingcom

Glossary (https://www.bleepingcomputer.com/

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)