FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

19 NOV 2020

Alert Number

MU-000139-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Cyber Actors Target Misconfigured SonarQube Instances to Access Proprietary Source Code of US Government Agencies and Businesses

UPDATE: This report is an update to the FLASH released on 14 October 2020, Alert Number MU-000136-MW. The FLASH has been updated to include additional technical details and a blog post by SonarQube addressing this issue.

Summary

Since April 2020, unidentified cyber actors have actively targeted vulnerable SonarQube instances to access source code repositories of US government agencies and private businesses. The actors exploit known configuration vulnerabilities, allowing them to gain access to proprietary code, exfiltrate it, and post the data publicly. The FBI has identified multiple potential computer intrusions that correlate to leaks associated with SonarQube configuration vulnerabilities.

Technical Details

SonarQube is a web-based, open-source platform used to measure and analyze source code quality. This service performs automatic reviews of code to detect bugs and security vulnerabilities on 20+ programming languages. It conducts continuous code inspection and issues alerts of potential flaws, bugs, and security vulnerabilities during the development of an application.

Beginning in April 2020, the FBI observed source code leaks associated with insecure SonarQube instances from US government agencies and private US companies in the technology, finance, retail, food, eCommerce, and manufacturing sectors.

In August 2020, unknown threat actors leaked internal data from two organizations through a public lifecycle repository tool. The stolen data was sourced from SonarQube instances that used default port settings and admin credentials running on the affected organizations' networks. This activity is similar to a previous data leak in July 2020, in which an identified cyber actor exfiltrated proprietary source code from enterprises through poorly secured SonarQube instances and published the exfiltrated source code on a self-hosted public repository.

During the initial attack phase, cyber actors scan the internet for SonarQube instances exposed to the open Internet using the default port (9000) and a publicly accessible IP address. Cyber actors then use default administrator credentials (username: admin, password: admin) to attempt to access SonarQube instances.

On 31 July 2020, SonarQube released a blog post addressing this issue, which can be accessed at https://blog.sonarsource.com/public-response-colde-leaks.

Recommended Mitigations

- Change the SonarQube default settings, including changing default administrator username, password, and port (9000).
- Place SonarQube instances behind a login screen, and check if unauthorized users have accessed the instance.
- Revoke access to any application programming interface keys or other credentials that were exposed in a SonarQube instance, if feasible.

- Configure SonarQube instances to sit behind your organization's firewall and other perimeter defenses to prevent unauthenticated access.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.