SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

Many Prometheus Endpoints Expose Sensitive Data

By Ionut Arghire on October 18, 2021

Unprotected instances of open source event monitoring solution Prometheus may leak metric and label data to the Internet, software company JFrog warns.

Designed to harvest real-time metrics from various endpoints, Prometheus enables organizations to keep a close eye on systems' state, network usage, and the like. Close to 800 cloud-native platforms, including Slack and Uber, leverage the solution.

In January 2021, Prometheus added support for Transport Layer Security (TLS) and basic authentication, to prevent access to the captured metrics. However, numerous Prometheus endpoints that are accessible from the Internet were found to leak metric and label data, JFrog reveals.

Prometheus, the software company says, has long avoided built-in support for security features, to focus on monitoring-related features, which has resulted in the leak of many types of sensitive data, of which developers often had no clue.

JFrog performed "a large-scale unauthenticated scraping of publicly available and non-secured Prometheus endpoints," which by default allow for untrusted, public access.

This means that most publicly-exposed Prometheus endpoints could be accessed from the Internet without authentication, and JFrog found nearly 27,000 of them using Shodan, and 43,000 hosts

using ZoomEye.

Some of the exposed data includes addresses of targets and services and usernames for accessing them, credentials in URL strings, infrastructure services, machine addresses and metadata labels, SSH public keys, environment variables for Kubelet, and more.

Non-secure deployments of Prometheus, JFrog warns, may pose an even larger security risk, via an optional management API that can be used to delete metrics and close the monitoring server. Roughly 15 percent of the identified exposed Prometheus endpoints had the API management feature enabled (it is disabled by default).

“This means that right off the bat, an unauthenticated attacker can trivially shutdown and/or delete the metrics of these Prometheus endpoints,” JFrog notes.

Basic authentication capabilities and TLS support were added in Prometheus version 2.24.0, and developers and organizations are advised to update to that or newer versions of the monitoring solution, to prevent sensitive data leaks.

“We highly recommend using authentication and encryption mechanisms when deploying Prometheus to help secure against the inadvertent leakage of sensitive information. Implementing these features in Prometheus 2.24.0 and later versions is easier than ever due to the built-in support that was added by the Prometheus team in January,” JFrog notes.

Related: **FBI Reportedly Exposed Secret Terrorist Watchlist**

Related: **ImmuniWeb Launches Free Tool for Identifying Unprotected Cloud Storage**

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Many Prometheus Endpoints Expose Sensitive Data

Accenture Confirms Data Stolen in Ransomware Attack

Russia-Linked TA505 Back at Targeting Financial Institutions

Deepfence Open Sources Vulnerability Mapping Tool 'ThreatMapper'

VirusTotal Shares Analysis of 80 Million Ransomware Samples

Tags:

NEWS & INDUSTRY Vulnerabilities Data Protection