KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Unauthenticated Redis Instances Exposed on the Internet

Tracker ID: TN1001 **Date:** 06/Oct/2022 **Category:** Incident **Industry:** All **Region**: All

Background

An unidentified attacker was seen attempting to install a cryptocurrency miner on tens of thousands of exposed unauthenticated Redis servers. The attack was made possible by a "lesser-known method" designed to trick servers into writing data to random files. The prime intention of this exploitation technique is to configure Redis to write its file-based database to a directory containing a mechanism to start a process (such as adding a script to "/etc/cron.d") or authorize a user (such as adding a key to ".ssh/authorized keys").

The detected Redis commands indicated that a shell script stored on a remote server was executed as a result of the attacker's attempts to store malicious crontab entries in the file "/var/spool/cron/root." The shell script is intended to terminate security-related and system monitoring procedures, delete log files and command histories, enable remote access, and add a new SSH key ("backup1") to the root user's authorised keys file. It also installed scanning programs such as masscan, switched off the iptables firewall, and started the XMRig cryptocurrency mining program.

Out of the 31,239 unauthenticated Redis servers identified, 15,526 are said to have the SSH key set, implying that nearly 49% of those servers were the targets of the attack. The major reason this attack may fail is that the Redis service requires root access to allow the adversary to write to the previously mentioned cron directory. When Redis is executed inside a container like Docker, the process could be tricked into allowing the attacker to write these files. In this case, the container is impacted, but the physical host is unaffected.

There are around 350,675 internet-accessible Redis database services distributed among 260,534 unique servers. 11% (or 39,405) of these services are not authenticated. The potential data exposure from the 39,405 unauthenticated Redis servers discovered exceeds 300 gigabytes. There have been multiple reports of poorly setup Redis services, with Israel being one of the few countries where the number of incorrectly configured Redis servers outnumbers the number of properly configured ones. Almost half of unauthenticated Redis services on the Internet exhibit signs of a breach attempt.

The top 10 countries with unauthenticated and exposed Redis services are China (20,011), the United States (5,108), Germany (1,724), Singapore (1,236), India (876), France (807), Japan (711), Hong Kong (512), the Netherlands (433), and Ireland (390). Redis is optimized for performance and simplicity rather than security. It is not recommended to be exposed directly to the Internet or in an environment where untrusted clients can access the Redis TCP port or UNIX socket. Redis servers, whether infected or not, contain unencrypted private SSH keys and certificates that can be exploited to gain access to servers and decode network traffic as well as PII and other sensitive data. Thus, Redis should be available only to trustworthy clients in trusted environments.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Unauthenticated Redis Instances Exposed on the Internet

Tracker ID: TN1001 **Date:** 06/Oct/2022 **Category:** Incident **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Privilege Escalation and Execution.

Recommendations

- Enable client authentication in Redis configuration file and configure Redis to only run on internal-facing network interfaces.
- Configure your firewall only to accept Redis connections from trusted hosts.
- To avoid configuration abuse, disable the “CONFIG” command by renaming it to a unique and unguessable command using ‘rename-command CONFIG “”’.
- It is advised to constantly monitor the services and critical assets that are exposed to the Internet

References

- Ravie Lakshmanan, Over 39,000 Unauthenticated Redis Instances Found Exposed on the Internet, The Hacker News, 21st September 2022, External Link (thehackernews.com)
- Databases. EXPOSED! (Redis), Censys, 21st September 2022, External Link (censys.io)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471