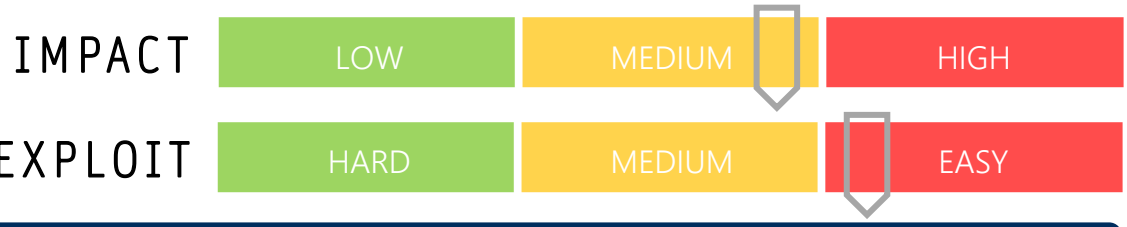
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00080

PGMINER INNOVATIVE NEW BOTNET DISCOVERED

DATE ISSUED: 15th December 2020



OVERVIEW

The discovery of a Linux-based Monero cryptomining botnet uses pioneering techniques to target PostgreSQL database servers pursuing a Remote Code Execution (RCE) vulnerability using novel PGMiner malware.

BREAKDOWN

PostgreSQL servers, an open-source relational database management system for production environments, are the target under exploitation through the vulnerability CVE-2019-9193 and is the first malware known to actively target this type of system. The feature 'copy from program' may be exploited to allow a local or remote user with superuser privileges to run shell scripts directly on the server. the attacker can scan port 5432 with a randomly chosen public network address range and once discovered, use static links to access the client library to scan for target databases that can then be subjected to brute force password attacks. Once compromised, the attacker may then elevate their privileges and execute the coin mining malware by a fileless approach and removing the table after scripts are launched and using 'curl' to carry out various commands. Following this, a link to the Command and Control (C2) server is established via SOCKS5 proxies and system information is exfiltrated to determine the most suitable payload for download. It will then perform clean-up steps to avoid detection. The aforementioned CVE is currently disputed by the PostgreSQL community.

REMEDIATION STEPS

- Ensure superuser privileges are not given to remote or untrusted users
- Ensure access controls and authentication mechanisms are in place and properly configured

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/pgminer-monero-mining-botnet/162209/
Palo Alto: https://unit42.paloaltonetworks.com/pgminer-postgresql-cryptocurrency-mining-botnet/
Security Week: https://www.securityweek.com/pgminer-crypto-mining-botnet-abuses-postgresql-distribution
ZDNet: https://www.zdnet.com/article/pgminer-botnet-attacks-weakly-secured-postgresql-databases/