Severity

High

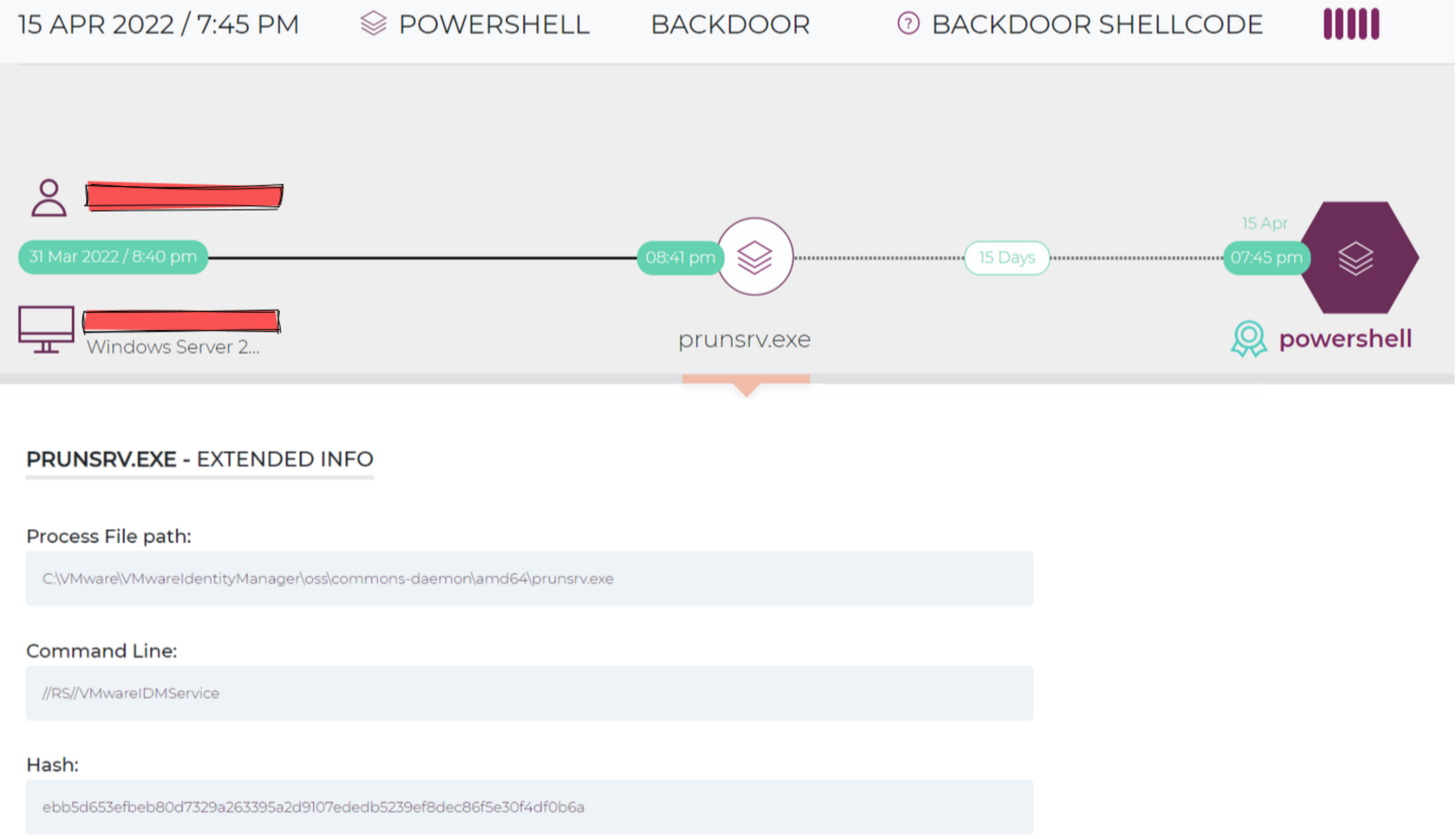
Analysis Summary

Security researchers identified exploitation attempts for a week-old VMware Workspace ONE Access vulnerability. A malicious actor exploiting this vulnerability potentially gains an unlimited attack surface. Security breaches, ransom, brand harm, and lawsuits are all possible outcomes for affected organizations. The attack's tactics, techniques, and procedures are similar to those utilized by groups like the Iranian-linked Rocket Kitten.

This new vulnerability is a server-side template injection that affects an Apache Tomcat component and executes a malicious command on the hosting server. A hostile actor with network access can exploit this vulnerability to acquire full remote code execution against VMware's identity access management.

According to research, attackers are already exploiting this vulnerability to launch reverse HTTPS backdoors, mainly Cobalt Strike, Metasploit, or Core Impact beacons.. With privileged access, these sorts of attacks may be able to circumvent standard defenses such as antivirus (AV) and endpoint detection and response (EDR).

Security researchers have analyzed this new attack in detail below.



PRUNSRV.EXE - EXTENDED INFO

Process File path:

C:\VMware\VMwareIdentityManager\oss\commons-daemon\amd64\prunsrv.exe

Command Line:

//RS//VMwareIDMService

Hash:

ebb5d653efbeb80d7329a263395a2d9107ededb5239ef8dec86f5e30f4df0b6a

Another VMWare component, the VMWare Identity Manager service, is now exploited by threat actors. Several vulnerabilities have recently been reported, including CVE-2022-22957, CVE-2022-22958, and CVE-2022-22954.

- CVE-2022-22957 and CVE-2022-22958 are RCE vulnerabilities that require administrative access to the server.
- CVE-2022-22954 already has an open-source proof of concept in the wild.

Impact

- Security Bypass
- Remote Code Execution
- Cross-Site Scripting
- Privilege Escalation
- Information Disclosure

Indicators Of Compromise

CVE

- CVE-2022-22957
- CVE-2022-22958
- CVE-2022-22954

IP

- 185[.]117[.]90[.]187

MD5

- 19d88d7db3b7594c13bf4071632a5013

SHA-256

- 746ffc3bb7fbe4ad229af1ed9b6e1db314880c0f9cb55aec5f56da79bce2f79b

SHA-1

- f42cd7c024969b8b589620b0643e0d974a95c84d

Affected Vendors

- VMware

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.

Refer to VMware Security Advisory for the patch, upgrade or suggested workaround information.

VMware Security Advisory