Hive Pro

THREAT ADVISORY

Newly patched VMware vulnerability exploited by Iranian espionage group, Rocket Kitten	TA2022101

Threat Level	RED	Publish Date – April 26, 2022

An Iranian cyber espionage gang known as Rocket Kitten has began delivering the Core Impact penetration testing tool on susceptible computers by exploiting a newly fixed severe vulnerability in VMware Workspace ONE Access/Identity Manager program.

Threat actors use the VMWare Identity Manager Service flaw (CVE-2022-22954) to acquire initial access to a target system, then install a PowerShell stager to download the next stage payload, nicknamed PowerTrash Loader. The PowerTrash Loader is a 40,000-line PowerShell script that has been substantially obfuscated. PowerTrash Downloader introduces the penetration testing framework Core Impact to memory at the end of the attack chain.

The MITRE ATT&CK TTPs commonly used by Rocket Kitten are:
TA0001: Initial Access
TA0002: Execution
TA0006: Credential Access
TA0009: Collection
TA0011: Command and Control
T1059 - Command and Scripting Interpreter
T1189 - Drive-by Compromise
T1555.003: Credentials from Password Stores: Credentials from Web Browsers
T1105: Ingress Tool Transfer
T1056.001: Input Capture: Keylogging
T1566.001: Phishing: Spearphishing Attachmet
T1566.003: Phishing: Spearphishing via Servicen
T1204.002: User Execution: Malicious File

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
Rocket kitten (Newscaster, NewsBeef, Parastoo, Group 83)	Iran	Worldwide	Construction, Defense, Education, Embassies, Entertainment, Government, Manufacturing, Media.	Information theft and espionage

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE
CVE-2022-22954	VMware Workspace ONE Access versions 20.10.0.0 - 21.08.0.1; vRealize Suite Lifecycle Manager versions 8.0 - 8.4.1 Patch 2; VMware Cloud Foundation versions 4.0 - 4.3.1.1; VMware Identity Manager versions 3.3.3 - 3.3.6	cpe:2.3:a:vmware:vmware_workspace_one_access:*:*:*:*:*:*:*:*,cpe:2.3:a:vmware:vrealize_suite_lifecycle_manager:*:*:*:*:*:*:*:*,cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*,cpe:2.3:a:vmware:identity_manager:*:*:*:*:*:*:*:*	Server-side Template Injection Remote Code Execution Vulnerability	CWE-94

Indicators of Compromise (IoCs)

Type	Value
MD5	19d88d7db3b7594c13bf4071632a5013
IPV4	185.117.90[.]187 138.124.184[.]220
SHA1	f42cd7c024969b8b589620b0643e0d974a95c84d
SHA256	746ffc3bb7fbe4ad229af1ed9b6e1db314880c0f9cb55aec5f56da79bce2f79b, 7bc14d231c92eeeb58197c9fca5c8d029d7e5cf9fbfe257759f5c87da38207d9
URL	hxxp://138.124.184[.]220/work_443.bin_m2.ps1

Patch Links

https://www.vmware.com/security/advisories/VMSA-2022-0011.html

References

https://blog.morphisec.com/vmware-identity-manager-attack-backdoor