NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

November 2021, Edition 1.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and security patch advisory. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
Arbitrary file read and SSRF vulnerabilities in the vCenter Server products were more likely to be exploited in hacking campaigns.	High
RedCurl cyberespionage group resumed targeting organizations across various industries.	High
Threat actors were leveraging domain fronting techniques to target the Myanmar government.	High
Privilege escalation vulnerability (CVE-2021-22048) in VMware vCenter Server were more likely to exploit hacking campaigns.	High

ALSO INSIDE

Security Patch Advisory

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Arbitrary file read and SSRF vulnerabilities in the vCenter Server products were more likely to be exploited in hacking campaigns.

Severity: High

Date: November 25, 2021

BUSINESS IMPACT

Successful exploitation of vulnerabilities allow remote unauthenticated attacker to read arbitrary files on the system, gain access to sensitive information and send malicious requests to other servers from the vulnerable system.

RECOMMENDATIONS

1. Update VMware vCenter Server to latest versions 6.7 U3p & 6.5 U3r.

2. Ensure to apply security patches on vulnerable VMware Cloud Foundation as soon as patches released.

INTRODUCTION

Arbitrary file read vulnerability (CVE-2021-21980) exists in the vSphere Web Client (FLEX/Flash). The vulnerability exists due to input validation errors when processing directory traversal sequences. A remote attacker with network access to port 443 on vCenter Server can send a specially crafted HTTP request and read arbitrary files on the system. The vulnerability allows a remote attacker to perform directory traversal attacks.

The vSphere Web Client (FLEX/Flash) contains an SSRF (Server-Side Request Forgery) vulnerability (CVE-2021-22049) in the vSAN Web Client (vSAN UI) plug-in that allows a remote attacker to perform SSRF attacks. The vulnerability exists due to insufficient validation of user-supplied input. A remote attacker with network access to port 443 on vCenter Server can send a specially crafted HTTP request and trick the application to initiate requests to arbitrary systems. Successful the exploitation of this vulnerability may allow a remote attacker to gain access to sensitive data in the local network or send malicious requests to other servers from the vulnerable system.

AFFECTED COMPONENTS

- VMware vCenter Server versions 6.7 and 6.5
- VMware Cloud Foundation version 3.x

READ

- VMware addresses File Read and SSRF flaws in vCenter Server

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

RedCurl cyberespionage group resumed targeting organizations across various industries.

Severity: High

Date: November 22, 2021

REMEDIATION

1. Ensure Microsoft Windows Servers and Workstations are updated with the latest security patches.
2. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
3. Ensure Domain Accounts follows the least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
4. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through a VPN tunnel.
5. Ensure VPN client software and VPN servers are patched with the latest security updates released by the vendor.
6. Set PowerShell execution policy to execute only signed scripts. The change in policy on a system may be a way to detect malicious use of PowerShell.
7. Implement unauthorized execution prevention by disabling macro scripts from Microsoft Office files, monitor and/or block inbound connections from Tor exit nodes and other anonymization services.
8. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
9. Do not click on links or download untrusted email attachments coming from unknown email addresses.
10. Educate employees about phishing attacks and use effective email filtering techniques from external sources.
11. Limit unnecessary lateral communications between network hoses, segments, and devices.
12. Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
13. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.
14.Kindly block the threat indicators at their respective controls.

READ

- RedCurl corporate espionage hackers resume attacks with updated tools
- RedCurl hacking group returns with new attacks

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
f635be0fc6ff1faf55a60fde5b3a0f273f1c8ed622e6915b9a2fb4ae0085b1d8	Not Known	Not Known	Not Known	Not Known	Not Known
b850c56109ba9ecadd5a6af3b764482cc814f7adba24d5a5c60a710e97f2b65f	Yes	Yes	Yes	Yes	No
c0f04cefd10f1e65f342d9456a3cab4b2b1aab6523a4789147e6ef556a7e8585	Not Known	Not Known	Not Known	Not Known	Not Known
12ae4ed672f495619fa480477d4b83d058ad3764ecaf86cd490cd3ea689158bc	Not Known	Not Known	Not Known	Not Known	Not Known
2cbdda564a8e2cbcffdbab89b978cba561d42da1889de7c817d8e0cd663c3322	Not Known	Not Known	Not Known	Not Known	Not Known
cceef032c86d7ebac083c6506506fee8dd83475a10853e11bb133d2ec70115fe	Yes	Yes	Yes	Yes	No
00d10d276f3684787302a826c44718af77ff41020e2fbaed24fbec893e1f2004	Not Known	Not Known	Not Known	Not Known	Not Known

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat actors were leveraging domain fronting techniques to target the Myanmar government.

Severity: High

Date: November 17, 2021

IP ADDRESSES

193.135.134[.]124

DOMAINS

test.softlemon[.]net
dark-forest-002.president.workers[.]dev

URLS

hxxp://test.softlemon[.]net:8081/api/3
hxxp://test.softlemon[.]net/
tcp://test.softlemon[.]net:8080/
hxxps://193.135.134[.]124:8443
hxxp://193.135.134[.]124:8080
hxxp://193.135.134[.]124:8081

REMEDIATION

1. Ensure Microsoft Windows Servers and Workstations are patched with the latest
security updates.
2. Ensure Microsoft Exchange Servers are updated with the latest security patches.
3. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.
4. Ensure network segments that allow communication over TCP port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are strictly monitored for any anomaly or suspicious patterns like lateral movement, excessive network traffics on TCP port 135, TCP Port 445, TCP Port 1900, TCP Port 3389, and an unusual amount of data transmission, etc.
5. Ensure Domain Accounts follows the least privilege principle and ensure two-factor authentication is enabled on all Business Email Accounts.
6. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through a VPN tunnel.
7. Ensure VPN client software and VPN servers are patched with the latest security updates released by the vendor.
8. Strictly ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are not left open on the Internet or DMZ facing side.
9. Please ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389, are only accessible through VPN tunnels between VPN clients and the organization's resources.
10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
11. Ensure to monitor for excessive LDAP queries within 5 minutes from particular the system, via SIEM solution.
12. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.
13. Ensure data backup is done periodically and ensure data backups are done via an out-of-band network onto the server with limited or no internet access.
14. Kindly Block Domains, URLs, and Hashes on the perimeter security devices.

READ

- Attackers use domain fronting technique to target Myanmar with Cobalt Strike

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Privilege escalation vulnerability (CVE-2021-22048) in VMware vCenter Server were more likely to exploit hacking campaigns.

Severity: High

Date: November 11, 2021

BUSINESS IMPACT

Successful exploitation of vulnerability allows remote attacker with non-administrative access to vCenter Server to elevate privileges to a higher privileged group, take control of a company's affected system, deploy further malicious payload to execute ransomware like disruptive attacks.

WORKAROUND

1. Switch SSO identity source configuration from Integrated Windows Authentication (IWA) to AD over LDAPS authentication/Identity Provider Federation for AD FS (vSphere 7.0 only) as documented in the KB86292.

RECOMMENDATIONS

1. Ensure to apply security patches on vulnerable VMware Cloud Foundation & vCenter Server as soon as patches released.

INTRODUCTION

Privilege escalation vulnerability (CVE-2021-22048) existing in VMware vCenter Server allows a remote user to escalate privileges on the system.

The vulnerability exists due to an error in the IWA (Integrated Windows Authentication) authentication mechanism. Attackers with nonadministrative access to vCenter Server may exploit this issue to elevate privileges to a higher privileged group.

VMware has yet to fix the vulnerability and is more likely to be actively exploited by threat actors in the wild.

CVSSv3 score: 7.1

AFFECTED COMPONENTS

- VMware vCenter Server versions 6.7 and 7.0
- VMware Cloud Foundation versions 3.x and 4.x

READ

- VMware discloses a severe flaw in vCenter Server that has yet to fix

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

8th November to 14th November | Trac- ID: NII21.11.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
November 11 2021	Ubuntu Linux	USN-5146-1: Thunderbird vulnerabilities	• Ubuntu 21.04 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
November 11 2021	Red Hat Enterprise Linux	RHSA-2021:4622 - Security Advisory	▪ Red Hat Enterprise Linux for x86_64 8 x86_64 ▪ Red Hat Enterprise Linux for ARM 64 8 aarch64	Kindly update to fixed version
November 11 2021	Red Hat Enterprise Linux	RHSA-2021:4620 - Security Advisory	▪ Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.1 x86_64 ▪ Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.1 aarch64	Kindly update to fixed version

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

8th November to 14th November | Trac- ID: NII21.11.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
November 11, 2021	Oracle Linux	ELSA-2021-9545 - httpd:2.4 security update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64	Kindly update to fixed version
November 11, 2021	Oracle Linux	ELSA-2021-4619 - freerdp security update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64)	Kindly update to fixed version

CITRIX

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
November 09 2021	Citrix ADC and Citrix Gateway	Citrix Application Delivery	▪ Citrix ADC and Citrix Gateway 13.0 before 13.0-83.27 ▪ Citrix ADC and Citrix Gateway 12.1 before 12.1-63.22 ▪ Citrix ADC and NetScaler Gateway 11.1 before 11.1-65.23 ▪ Citrix ADC 12.1-FIPS before 12.1-55.257	Kindly update to fixed version