NETWORK INTELLIGENCE

Digest

May 2022, 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
The zero-day bug in Microsoft Office Products allows remote code execution	● Critical
Multiple vulnerabilities in Google Chrome more likely to be exploited in targeted hacking campaigns & malware attacks	● Critical
Critical vulnerabilities tracked as CVE-2022-22972 and CVE-2022-22973 impact multiple VMware products	● Critical
Critical BIG-IP Remote Code Execution Vulnerability could lead to a complete system takeover	● Critical

ALSO INSIDE

Security Patch Advisory

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

The zero-day bug in Microsoft Office Products allows remote code execution.

Severity: Critical

Date: May 30, 2022

BUSINESS IMPACT

Successful exploitation of the vulnerability allows a remote attacker to compromise a vulnerable system, execute arbitrary code and launch malware or ransomware attacks.

MITIGATION MEASURES

1. Use Microsoft Defender's Attack Surface Reduction (ASR) to activate the rule "Block all Office applications from creating child processes" in Block mode to prevent vulnerability exploitation.

2. The vulnerability exploitation can be blocked by removing the handler. Remove the file type association for ms-msdt (can be done in Windows Registry HKCR:\ms-msdt or with Kelvin Tegelaar's PowerShell snippet).

This measure will block the ability of the Office to invoke ms-msdt thus preventing the malware from running. Be sure to make a backup of the registry settings before using this mitigation.

INTRODUCTION

The security researchers have discovered a zero-day flaw in Microsoft Office Products dubbed Follina. The vulnerability has been exploited in the wild since April 2022, and it's likely to see more exploitation attempts in the wild through email-based delivery. Follina is a zero-click remote code execution technique that leverages MSDT (Microsoft Diagnostics Tool) and Microsoft Office utilities.

The exploitation attempts involve delivering emails containing office documents. The document uses the Word remote template feature to retrieve an HTML file from a remote web server, which uses the ms-msdt MSProtocol URI scheme to load malicious code and execute PowerShell. The attacks can also use the Rich Text Format file (.rtf) to trigger the invocation of this vulnerability with just the Preview Pane within Windows Explorer to bypass Protected View and execute the code. Successful exploitation spawns' processes under sdiagnhost.exe.

AFFECTED PRODUCT

The issue affects multiple Microsoft Office versions.

DETECTION

1. Use Sigma rule to detect the execution of weaponized maldoc or embedded link in outlook that uses ms-msdt scheme to execute code.

2. Use Yara rule to detect suspicious msdt.exe execution to identify ongoing Office/Msdt exploitation.

3. Defender for Endpoint users can use Advanced Hunting Query to hunt for Follina MSDT attacks.

REFERENCES

- Follina — a Microsoft Office code execution vulnerability
- Microsoft Office Remote Code Execution – "Follina" MSDT Attack

Multiple vulnerabilities in Google Chrome more likely to be exploited in targeted hacking campaigns & malware attacks

Severity: Critical

Date: May 25, 2022

BUSINESS IMPACT

Successful exploitation of the vulnerabilities allows a remote attacker to compromise a vulnerable system, trigger use-after-free error, execute arbitrary code, bypass implemented security restrictions, trigger out-of-bounds read error and gain access to potentially sensitive information.

RECOMMENDATIONS

1. Kindly update Google Chrome browser for Windows to the latest release 102.0.5005.61/62/63 or later.

2. Kindly update Google Chrome browser for Mac and Linux to the latest release 102.0.5005.61 or later.
To verify if the Chrome browser is running latest release, go to Chrome menu > Help > About Google Chrome.

3. Ensure to update Chromium-based browsers such as Microsoft Edge, Opera, and Vivaldi to their latest releases as and when they become available.

INTRODUCTION

Google has released an update to its Chrome browser for Windows/macOS/Linux that address **32** security fixes. The latest Chrome update fixes 1 critical (CVE-2022-1853) and 8 high (CVE-2022-1854, CVE-2022-1855, CVE-2022-1856, CVE-2022-1857, CVE-2022-1858, CVE-2022-1859, CVE-2022-1860, CVE-2022-1861) severity vulnerabilities.

CVE-2022-1853 is a use-after-free bug within the Indexed DB component in Google Chrome.

CVE-2022-1854 is a use-after-free bug within the ANGLE ("a graphics engine abstraction layer") in Google Chrome.

CVE-2022-1855 is a use-after-free bug within the Messaging component in Google Chrome.

CVE-2022-1856 is a use-after-free bug within the User Education component in Google Chrome.

CVE-2022-1857 is an Insufficient policy enforcement bug in File System API in Google Chrome.

CVE-2022-1858 is an Out of bounds read bug in DevTools in Google Chrome.

CVE-2022-1859 is a use-after-free bug within the Performance Manager component in Google Chrome.

CVE-2022-1860 is a use-after-free bug within the UI Foundations component in Google Chrome.

CVE-2022-1861 is a use-after-free bug within the Sharing component in Google Chrome.

A remote attacker can trick the victim into visiting a specially crafted web page to trigger a use-after-free error or out-of-bounds read error or bypass implemented security measures and compromise the vulnerable system.

AFFECTED PRODUCT

Google Chrome browser (release prior to 102.0.5005.61) for Windows, Mac and Linux.

REFERENCES

- Stable Channel Update for Desktop

NETWORK INTELLIGENCE

SECURITY ADVISORY

Critical vulnerabilities tracked as CVE-2022-22972 and CVE-2022-22973 impact multiple VMware products

Severity: Critical

Date: May 19, 2022

BUSINESS IMPACT

Successful exploitation of vulnerabilities allows a malicious actor to bypass the authentication process, escalate privileges, obtain administrative access, execute arbitrary code with root privileges and obtain full system control of the affected application.

RECOMMENDATIONS

1. Update VMware Workspace ONE Access (Access), VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation, vRealize Suite Lifecycle Manager to latest security patches to address CVE-2022-22972 & CVE-2022-22973.

Patch instructions to address CVE-2022-22972, CVE-2022-22973 – Click here.

WORKAROUND

1. To temporarily mitigate the authentication bypass flaw (CVE-2022-22972) in cases where admins cannot patch their appliances immediately can apply the Workaround.

The Workaround require admins to disable all users except one provisioned administrator and log in via SSH to restart the horizon-workspace service.

Workaround instructions to address CVE- 2022-22972 – Click here.

INTRODUCTION

VMware has released patches to address critical authentication bypass flaw (CVE-2022-22972) and high severity local privilege escalation flaw (CVE-2022-22973) in multiple products.

1. Authentication Bypass Vulnerability (CVE-2022-22972) exists in VMware Workspace ONE Access, Identity Manager and vRealize Automation. The vulnerability exists due to an error in the UI when processing authentication requests. A remote attacker with network access to the UI can bypass the authentication process to obtain administrative access.

CVSS Score: 9.8

2. Local Privilege Escalation Vulnerability (CVE-2022-22973) exists in VMware Workspace ONE Access and Identity Manager. The vulnerability exists due to application does not correctly impose security restrictions. A local malicious user can exploit the vulnerability to elevate permissions on unpatched devices to 'root' and execute arbitrary code with root privileges.

CVSS Score: 7.8

The vulnerabilities are more likely to be exploited in targeted hacking campaigns & malware attacks to deploy coin miners and install backdoors.

AFFECTED PRODUCT

- VMware Workspace ONE Access Appliance versions 21.08.0.1, 21.08.0.0, 20.10.0.1, 20.10.0.0
- VMware Identity Manager Appliance versions 3.3.6, 3.3.5, 3.3.4, 3.3.3,
- VMware vRealize Automation version 7.6
- VMware Cloud Foundation (vIDM) versions 4.3.x, 4.2.x, 4.1, 4.0.x
- VMware Cloud Foundation (vRA) version 3.x
- vRealize Suite Lifecycle Manager (vIDM) version 8.x

REFERENCES

- VMware patches critical auth bypass flaw in multiple products
- VMware Workspace ONE Access, Identity Manager and vRealize Automationupdates address multiple vulnerabilities.

Critical BIG-IP Remote Code Execution Vulnerability could lead to a complete system takeover

Severity: Critical

Date: May 06, 2022

BUSINESS IMPACT

Successful exploitation of the flaw could permit an unauthenticated attacker to bypass authentication, execute arbitrary system commands, create or delete files, or disable services and take control of an affected system.

RECOMMENDATIONS

1. Update F5 BIG-IP products to latest security patches.

Patches for the iControl REST authentication bypass flaw have been introduced in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5.

NOTE: The branches of 12.x and 11.x will not receive a fixing patch.

MITIGATION

Following temporary mitigations can be used until the fixes can be applied. These mitigations restrict access to iControl REST to only trusted networks or devices, thereby limiting the attack surface.

- Block iControl REST access through the self IP address
- Block iControl REST access through the management interface
- Modify the BIG-IP httpd configuration

INTRODUCTION

F5 released patches to address remote code execution bug CVE-2022-1388, which allows undisclosed requests to bypass the iControl REST authentication in BIG-IP. An attacker could exploit CVE-2022-1388 to take control of an affected system.

The vulnerability exists in the iControl REST component due to a lack of authentication check. An unauthenticated attacker with network access to the BIG-IP systems through the management port and/or self IP addresses can exploit the vulnerability to execute arbitrary system commands, create or delete files, or disable services. There is no data plane exposure; this is a control plane issue only.

The vulnerability poses a significant risk of allowing threat actors to gain initial access to corporate networks. There are 16K+ F5 BIG-IP devices publicly exposed to the Internet. Most of these devices are located in the USA, followed by China, India, Australia, and Japan. The vulnerability is more likely to be exploited in targeted hacking campaigns & malware attacks.

CVSS Score: 9.8

AFFECTED PRODUCT

The vulnerability affects all modules of BIG-IP products with the following versions:

- 16.1.0 - 16.1.2
- 15.1.0 - 15.1.5
- 14.1.0 - 14.1.4
- 13.1.0 - 13.1.4
- 12.1.0 - 12.1.6
- 11.6.1 - 11.6.5

REFERENCES

- F5 Warns of a New Critical BIG-IP Remote Code Execution Vulnerability
- K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388

Security Patch Advisory

16th May to 22nd May | TRAC-ID: NII22.05.0.4

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
16-May-22	Ubuntu Linux	USN-5421-1: LibTIFF vulnerabilities	• Ubuntu 21.10 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 ESM • Ubuntu 14.04 ESM	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
18-May-22	Red Hat Enterprise Linux	RHSA-2022:4655	• Red Hat Enterprise Linux Server 7 x86_64 • Red Hat Enterprise Linux for Power, little endian 7 ppc64le	Kindly update to fixed version
18-May-22	Red Hat JBoss Middleware	RHSA-2022:4644	• Red Hat Enterprise Linux for Real Time 7 x86_64 • Red Hat Enterprise Linux for Real Time for NFV 7 x86_64	Kindly update to fixed version

NETWORK INTELLIGENCE

Security Patch Advisory

16th May to 22nd May | TRAC-ID: NII22.05.0.4

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

CISCO

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
21-May-22	Oracle Linux	ELSA-2022-9412	Oracle Linux 7 (x86_64)	Kindly update to fixed version
21-May-22	Oracle Linux	ELSA-2022-9409	• Oracle Linux 7 (aarch64) • Oracle Linux 7 (x86_64) • Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64)	Kindly update to fixed version