NETWORK INTELLIGENCE
The Digital Security Company

December 2022, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- 🟡 New ransomware families - Putin Team, ScareCrow, BlueSky, Meow, Vohuk and AERST
- 🔴 Critical vulnerabilities in multiple VMware products
- 🟡 A new Linux flaw (CVE-2022-3328) lets attackers gain root privileges & execute arbitrary code
- 🟡 Zero-day RCE flaw (CVE-2022-4262) in Google Chrome browser actively exploited in the wild

Also Inside

Security Patch Advisory

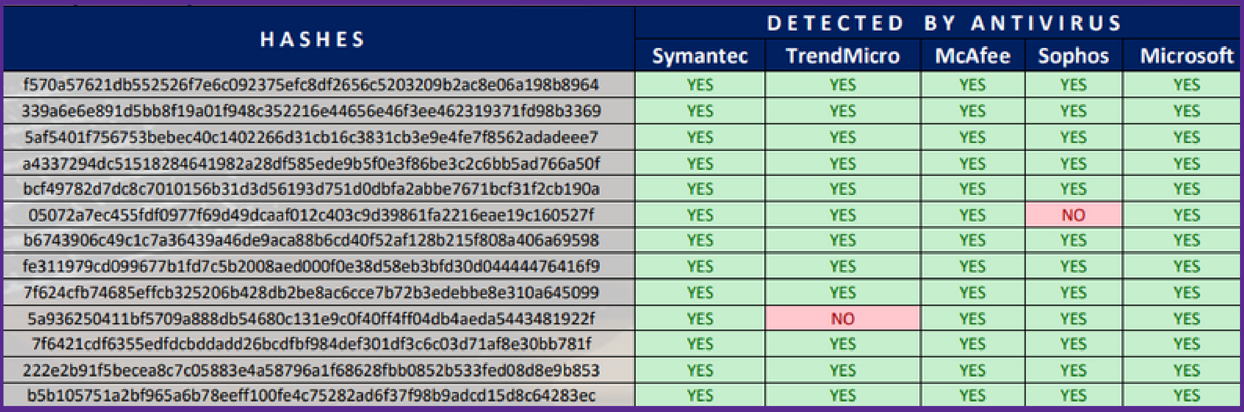
🔴 Critical 🟡 High 🟢 Low

Date: December 23, 2022

New ransomware families - Putin Team, ScareCrow, BlueSky, Meow, Vohuk and AERST

RECOMMENDATIONS

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with latest security patches.
3. Ensure anti-virus and endpoint detection products are up to date with the latest signatures.
4. Refrain from opening untrusted links and email attachments without first verifying their authenticity.
5. Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
6. Avoid downloading files from unknown websites.
7. Use strong passwords and enforce multi-factor authentication wherever possible.
8. Enable Data Loss Prevention (DLP) Solutions on the employees' systems.
9. Keep all systems and software updated to latest patched versions.
10.Prior to allowing VPN connections from remote endpoints, ensure that posture checking is configured to enforce a baseline set of security controls.
11. Ensure that the management interface of network devices is not exposed to the internet.
12.Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs.
13.Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
14.Use smart cards (tokens) or one-time codes as the second authentication factor when establishing a VPN connection. In cases where this is applicable, use the Access Control List (ACL) technology to restrict the list of IP addresses from which a VPN connection can be initiated.



HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Sophos	Microsoft
f570a57621db552526f7e6c092375efc8df2656c5203209b2ac8e06a198b8964	YES	YES	YES	YES	YES
339a6e6e891d5bb8f19a01f948c352216e44656e46f3ee462319371fd98b3369	YES	YES	YES	YES	YES
5af5401f756753bebec40c1402266d31cb16c3831cb3e9e4fe7f8562adadeee7	YES	YES	YES	YES	YES
a4337294dc51518284641982a28df585ede9b5f0e3f86be3c2c6bb5ad766a50f	YES	YES	YES	YES	YES
bcf49782d7dc8c7010156b31d3d56193d751d0dbfa2abbe7671bcf31f2cb190a	YES	YES	YES	YES	YES
05072a7ec455fdf0977f69d49dcaaf012c403c9d39861fa2216eae19c160527f	YES	YES	YES	NO	YES
b6743906c49c1c7a36439a46de9aca88b6cd40f52af128b215f808a406a69598	YES	YES	YES	YES	YES
fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d04444476416f9	YES	YES	YES	YES	YES
7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099	YES	YES	YES	YES	YES
5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda5443481922f	YES	NO	YES	YES	YES
7f6421cdf6355edfdcbddadd26bcdfbf984def301df3c6c03d71af8e30bb781f	YES	YES	YES	YES	YES
222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853	YES	YES	YES	YES	YES
b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec	YES	YES	YES	YES	YES

REFERENCES

- New Ransomware Strains Emerging From Leaked Conti's Source Code
- **OWASSRF: CrowdStrike Identifies New Exploit Method for Exchange Bypassing ProxyNotShell Mitigations**

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

Date: December 15, 2022

Critical vulnerabilities in multiple VMware products

BUSINESS IMPACT

Successful exploitation of the vulnerability allows an unauthenticated, remote attacker to gain complete control over vulnerable devices, remotely perform arbitrary code execution, read arbitrary files and plant further malware for disruptive attacks.

WORKAROUND

For those who can't apply the security update for CVE-2022-31705 VMware recommends to remove the USB controller from the ESXi virtual machine, Workstation and Fusion instances.

RECOMMENDATIONS

1. Kindly update VMware ESXi, Workstation, Fusion, Cloud Foundation and vRealize Network Insight instances to the latest versions.

INTRODUCTION

VMware has released fixes to address three flaws (tracked as CVE-2022-31705, CVE-2022-31702 & CVE-2022-31703) in multiple products.

VMware ESXi, Workstation, and Fusion contain a Heap out-of-bounds write vulnerability (CVE-2022-31705) due to a boundary error within the USB 2.0 controller (EHCI). A local privileged user on the guest OS can trigger an out-ofbounds write and execute arbitrary code as the virtual machine's VMX process runs on the host.
CVSS Score: 9.3

vRealize Network Insight (vRNI) contains a command injection vulnerability (CVE-2022-31702) due to improper input validation within the vRNI REST API. An unauthenticated, remote attacker can pass specially crafted data to the affected REST API endpoint and execute arbitrary OS commands on the target system.
CVSS Score: 9.8

vRealize Network Insight (vRNI) contains a directory traversal vulnerability (CVE-2022-31703) due to an input validation error when processing directory traversal sequences within the vRNI REST API. A remote attacker can send a specially crafted HTTP request and read arbitrary files on the system.
CVSS Score: 7.5

AFFECTED PRODUCTS

- ESXi 8.0, 7.0
- Fusion 12.x
- Workstation 16.x
- Cloud Foundation 4.x/3.x
- vRealize Network Insight versions 6.2 to 6.7

REFERENCES

- VMware fixes critical ESXi and vRealize security flaws
- VMware fixed critical VM Escape bug demonstrated at Geekpwn hacking contest

SECURITY ADVISORY

Date: December 7, 2022

A new Linux flaw (CVE-2022-3328) lets attackers gain root privileges & execute arbitrary code

BUSINESS IMPACT

Successful exploitation of the vulnerability allows a local attacker to gain root privileges, execute arbitrary code and plant further malware for disruptive attacks.

RECOMMENDATIONS

1. Ensure Linux servers and workstations are updated with latest security patches.

INTRODUCTION

Researchers discovered a new vulnerability (tracked as CVE-2022-3328) in the snap-confine function on Linux operating systems.

The vulnerability exists due to a race condition within the must_mkdir_and_open_with_perms() function in the snapd snap-confine binary when preparing the private /tmp mount for a snap. A local malicious user can exploit this race condition by chaining it with older vulnerabilities in multipathd (CVE-2022-41973 & CVE-2022-41974), gain unauthorized access to sensitive information, and obtain full root privileges on the target system.

CVSS Score: 7.8

AFFECTED PRODUCTS

- Ubuntu 22.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 ESM
- All Debian Linux versions with snapd (Debian package): before 2.37.4-1+deb10u1, before 2.49-1+deb11u2

REFERENCES

- Snapd Race Condition Vulnerability in snap-confine's must_mkdir_and_open_with_perms() (CVE-2022-3328)
- A New Linux Flaw Lets Attackers Gain Full Root Privilege

SECURITY ADVISORY

Date: December 5, 2022

Zero-day RCE flaw (CVE-2022-4262) in Google Chrome browser actively exploited in the wild

BUSINESS IMPACT

Successful exploitation of the vulnerability allows a remote attacker to trigger a type confusion error, execute arbitrary code on the target system, and plant further malware for disruptive attacks.

RECOMMENDATIONS

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

2. 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, Mac and Linux to address actively exploited zero-day vulnerability tracked as CVE-2022- 4262.

The vulnerability exists due to a type confusion error within the V8 engine in Google Chrome. A remote attacker can create a specially crafted web page, trick the victim into visiting it, trigger a type confusion error and execute arbitrary code on the target system.

AFFECTED PRODUCTS

- Google Chrome versions prior to 108.0.5359.94 for Mac and Linux
- Google Chrome versions prior to 108.0.5359.94/.95 for Windows

REFERENCES

- Google Chrome emergency update fixes 9th zero-day of the year
- Stable Channel Update for Desktop

SECURITY ADVISORY

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

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

12th Dec 2022 – 18th Dec 2022
TRAC-ID: NII22.12.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-5772-1: QEMU vulnerabilities	• Ubuntu 22.10 • Ubuntu 22.04 LTS • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 ESM • Ubuntu 14.04 ESM	Kindly update to fixed version
Ubuntu Linux	USN-5773-1: Linux kernel (OEM) vulnerabilities	• Ubuntu 22.04 LTS	Kindly update to fixed version

SUSE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
SUSE Linux	SUSE-SU2022:4546-1	• SUSE Linux Enterprise Server 12-SP5	Kindly update to fixed version
SUSE Linux	SUSE-SU2022:4545-1	• SUSE Linux Enterprise Live Patching 12-SP5	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

28th Nov 2022 – 4th Dec 2022
TRAC-ID: NII22.12.0.1

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2022-10080	• Oracle Linux 8 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2022- 10072	• Oracle Linux 7 (aarch64) • Oracle Linux 7 (x86_64)	Kindly update to fixed version

TENABLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Tenable.ad	[R1] Tenable.ad Versions 3.29.4, 3.19.12 and 3.11.9 Fix One Vulnerability	• Tenable.ad 3.29.3 • Tenable.ad 3.19.8 - 3.19.11 • Tenable.ad 3.11.3 - 3.11.7	Kindly update to fixed version

SECURITY ADVISORY

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