NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

January 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
Financially motivated threat actor Earth Lusca found actively targeting organizations globally.	● High
Zero-day privilege escalation vulnerability – "RemotePotato0" found impacting all Windows versions.	● High
Critical authentication bypass vulnerability impacted Zoho ManageEngine Desktop Central and Desktop Central MSP.	● Critical
A new multi-platform backdoor named SysJoker actively targeted Windows, Linux, and macOS.	● High

ALSO INSIDE

Security Patch Advisory

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

Financially motivated threat actor Earth Lusca found actively targeting organizations globally.

Severity: High

Date: January 24, 2022

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
3. Do not click on links or download untrusted email attachments coming from unknown email addresses.
4. Inspect the sender email address in the header to ensure the address matches with the purported sender.
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. Keep all systems and software updated to the latest patched versions.
9. When possible, include hash values in manifest files to help prevent side-loading of malicious libraries.
10. 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.
11. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
12. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet-facing
cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
13. Educate employees about phishing attacks and use effective email filtering techniques from external sources.
14. Disable Windows Script Host. This will prevent users from running any scripts (including VBScript and JScript scripts) that rely on WSH.
15. Ensure that unnecessary ports and services are closed to prevent the risk of discovery and potential exploitation.

DOMAINS

dsyu.livehost[.]live
3VnwTuq9s.ithome[.]house
dust.dnslookup[.]services
5s2zm07ao.wikimedia[.]vip
coivo2xo.livehost[.]live
r1d3wg7xofs.livehost[.]live
www.getdns[.]gd
6czumi0fbg.symantecupd[.]com
cookiestest[.]ml
1dfpi2d8kx.wikimedia[.]vip
qqfinance[.]ml
5NcNt6z1.wikimedia[.]vip
lzfhome[.]xyz
7hln9yr3y6.symantecupd[.]com
ybk47i6z8q.wikimedia[.]vip
bm2l41risv.livehost[.]live
w01grw7gs.ithome[.]house
o56n1tosy.livehost[.]live
lmogv.dnslookup[.]services
mztfki9x.wikimedia[.]vip
smtp.nslookup[.]club
ok3x377v3f.symantecupd[.]com

READ

- Earth Lusca Hackers Aimed at High-Value Targets in Government and Private Sectors
- Earth Lusca Employs Sophisticated Infrastructure, Varied Tools and Techniques
- Delving Deep: An Analysis of Earth Lusca's Operations

Financially motivated threat actor Earth Lusca found actively targeting organizations globally.

Severity: High

Date: January 24, 2022

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
7aaf33bb2979262590932dcfd6902d09a3c0045d906570a15123fa12f8656171	Not Known	Not Known	Not Known	Not Known	Not Known
ececbed665469514ed8583a4928f9a524f00a9b9c3c042015717ea22614398e4	Not Known	Not Known	Not Known	Not Known	Not Known
b081db87c75b6aea905a62532cb40bc21bc7acebb7a0c6c601d993c76a8c6ce1	No	No	No	No	No
bb45df12b63e5b133e6cb622b174ad68bc95a5bce15f98eede56597d38401b27	Not Known	Not Known	Not Known	Not Known	Not Known
566152a2d86186dcfb28856b4ed0dfdb60e355d93ab693f7931201f75868fff0	No	No	No	No	No
e2e969efc2d688e01a9aa32d50176374af811a3324651fb03b7b848e06e0b677	Not Known	Not Known	Not Known	Not Known	Not Known
c0725296e8ab3d9d3c932ecf45588f39ef8fa7a310d31bfd05a061194f8eeb1e	Not Known	Not Known	Not Known	Not Known	Not Known
b151285b331ab2450e2f7387590b29348ebb6f34391d4b10958faea715027795	Not Known	Not Known	Not Known	Not Known	Not Known
b5577248f532c2939db023d279d625fa4c01e9ee68441fe90046d2b6e79ac1d7	Not Known	Not Known	Not Known	Not Known	Not Known
9ee8b7ab27830bf615ce82f4b4930d10b735837842dfdd1d7ed25a460f76b863	Not Known	Not Known	Not Known	Not Known	Not Known
b5577248f532c2939db023d279d625fa4c01e9ee68441fe90046d2b6e79ac1d7	Not Known	Not Known	Not Known	Not Known	Not Known

Zero-day privilege escalation vulnerability – "RemotePotato0" found impacting all Windows versions.

Severity: High

Date: December 18, 2022

BUSINESS IMPACT

Successful exploitation of the vulnerabilities would allow remote attackers to perform SSRF attacks, trigger denial of service (DoS) or bypass security policies, execute arbitrary code on the target system and allow attackers to take full control of an affected system.

RECOMMENDATIONS

1. Windows admins should either disable NTLM or configure the servers to block NTLM relay attacks using Active Directory Certificate Services (AD CS).
2. If NTLM must remain enabled, it is strongly recommended to enable protections such as SMB signing, LDAP signing, and channel binding.
3. For HTTP(S), remove all non-TLS-protected HTTP bindings (prefer SSL everywhere, particularly where NTLM is used) and configure Channel Binding Tokens validation by setting the tokenChecking attribute to a minimum of Allow (if not Require) as documented here.
4. For LDAP, set the Domain controller: LDAP server signing requirements Group Policy to Require signature for non-LDAPS LDAP connections as documented here.
5. Set the Domain controller: LDAP server channel binding token requirements Group Policy to a minimum of When Supported (if not Always) as documented here.
6. For SMB, you should configure SMB Signing by setting the Group Policy Digitally sign server communication (always) as documented here.
7. Remove or Disable Nego/NTLM instead use Kerberos
8. Relayed credentials are most likely over the SMB or RPC services, hence ensure ports 139 and 445 are not left open on Internet or DMZ facing side.

INTRODUCTION

RemotePotato0 (Relaying Potatoes) - a local privilege escalation vulnerability, impacts all Windows versions. The flaw exists in Windows RPC Protocol. To exploit the bug, some higher-privileged users must be logged in to the same Windows computer as the attacker at the same time.

RemotePotato0 can be exploited without requiring the target's interaction by relaying authentication to other protocols. A logged-in low-privileged attacker can trigger authenticated RPC/DCOM calls and relay the NTLM authentication to other protocols, which allows them to elevate privileges from user to domain administrator, likely allowing full domain compromise.

Note: The vulnerability was disclosed in April 2021 is yet to receive a CVE ID, and the current status of this vulnerability is "won't fix".

DETECTION

Use YARA rule to detect RemotePotato0.

AFFECTED PRODUCT

All versions of Microsoft Windows Workstation and Server products

READ

- Windows 'RemotePotato0' zero-day gets an unofficial patch
- Relaying Potatoes: Another Unexpected Privilege Escalation Vulnerability in Windows RPC Protocol
- Free Micropatches for "RemotePotato0", a "WON'T FIX" Local Privilege Escalation Affecting all Windows Systems
- Proof Of Concept (POC)

Critical authentication bypass vulnerability impacted Zoho ManageEngine Desktop Central and Desktop Central MSP.

Severity: Critical

Date: December 18, 2022

BUSINESS IMPACT

Successful exploitation of the vulnerability allows remote attacker to bypass the authentication process, gain unauthorized access, perform unauthorized actions on the vulnerable server and deploy further malicious payload to execute ransomware like disruptive attacks.

RECOMMENDATIONS

1. Update Desktop Central server & Desktop Central MSP server to the latest build - 10.1.2137.9 or higher.

2. Follow the security hardening guidelines for Desktop Central and Desktop Central MSP to ensure all the security controls are configured to keep network secure.

INTRODUCTION

Zoho fixed critical vulnerability (CVE-2021-44757) that affects Desktop Central, and Desktop Central MSP unified endpoint management (UEM) the solution is more likely to be exploited in targeted hacking campaigns and malware attacks. The vulnerability exists due to an error when processing authentication requests.

A remote attacker can bypass the authentication process and gain unauthorized access to the server. The flaw also allows threat actors to read unauthorized data or write an arbitrary zip file on the server.

AFFECTED PRODUCT

The security issue impacts Desktop Central server & Desktop Central MSP server builds prior to 10.1.2137.9

READ

- Zoho fixes a critical vulnerability (CVE-2021-44757) in Desktop Central solutions
- Zoho Releases Patch for Critical Flaw Affecting ManageEngine Desktop Central
- Zoho plugs another critical security hole in Desktop Central
- A critical security patch released in Desktop Central and Desktop Central MSP for CVE-2021-44757

A new multi-platform backdoor named SysJoker actively targeted Windows, Linux, and macOS.

Severity: High

Date: January 12, 2022

REMEDIATION

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 Linux servers and workstations are updated with latest security patches.
4. Do not click on links or download untrusted email attachments coming from unknown email addresses.
5. Inspect the sender email address in the header to ensure the address matches with the purported sender.
6. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
7. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.
8. Keep all systems and software updated to latest patched versions.
9. Use Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature to block regsvr32.exe from being used to bypass
application control.
10. 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.
11. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing
cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
12. Test and review everything downloaded before approving it for use. The packages typically include update-time scripts that run when you do the
update, so malware infections could be delivered as part of the update process.
13. Make sure right modules are being downloaded from right publisher. Even legitimate modules sometimes have names that clash, compete, or confuse.
14. Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
15. Limit unnecessary lateral communications between network hoses, segments, and devices.

READ

https[://]bookitlab[.]tech
https[://]winaudio-tools[.]com
https[://]graphic-updater[.]com
https[://]github[.]url-mini[.]com
https[://]office360-update[.]com
https[://]drive[.]google[.]com/uc?export=download&id=1-NVty4YX0dPHdxkgMrbdCldQCpCaE-Hn
https[://]drive[.]google[.]com/uc?export=download&id=1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu

READ

- ‘Fully Undetected’ SysJoker Backdoor Malware Targets Windows, Linux & macOS
- New SysJoker Backdoor Targets Windows, Linux, and macOS

Security Patch Advisory

17th January to 23rd January | Trac- ID: NII22.01.0.4

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
17-Jan-22	Ubuntu Linux	USN-5227-2: Pillow vulnerabilities	• Ubuntu 16.04 ESM • Ubuntu 14.04 ESM	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
17-Jan-22	Red Hat Enterprise Linux	RHSA-2021:5226 - Security Advisory	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux Workstation 7 x86_64 ▪ Red Hat Enterprise Linux Desktop 7 x86_64	Kindly update to fixed version
17-Jan-22	Red Hat Enterprise Linux	RHSA-2021:5227 - Security Advisory	▪ Red Hat Enterprise Linux Server - Extended Life Cycle Support 6 x86_64 ▪ Red Hat Enterprise Linux Server - Extended Life Cycle Support 6 i386	Kindly update to fixed version

Security Patch Advisory

17th January to 23rd January | Trac- ID: NII22.01.0.4

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
18-Jan-22	Oracle Linux	ELSA-2022-0143 - httpd security update	▪ Oracle Linux 7 (aarch64) ▪ Oracle Linux 7 (x86_64)	Kindly update to fixed version
18-Jan-22	Oracle Linux	ELSA-2022-0143 - httpd security update	▪ Oracle Linux 7 (aarch64) ▪ Oracle Linux 7 (x86_64)	Kindly update to fixed version

NETAPP

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
18-Jan-22	NetApp Products	CVE-2021-44716 Golang Vulnerability in NetApp Products	Cloud Insights Telegraf Agent	Kindly update to fixed version