NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

January 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 |
|---|---|
| The Microsoft Patch Tuesday – January 2021 | Critical |
| The xHunt campaign that continued to target Government, Defense, and Privately held organizations in the Middle East | High |
| North Korea-based APT37 Threat Actors that were found targeting the government organizations in South Korea with the RokRat malware | High |
| An Authentication Bypass vulnerability (CVE-2020-10148) in Solarwinds Orion which allowed remote command execution from unauthenticated remote attackers | Critical |

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

# The Microsoft Patch Tuesday – January 2021

Severity: Critical

Date: January 14, 2021

## IMPACT

On successful exploitation of these vulnerabilities would allow remote attacker to execute malicious code in context of user account and take ownership of the affected Microsoft Products.

## REMEDIATION

1. Kindly apply available Microsoft patches on Microsoft Windows Workstations & Servers.

2. Kindly refer Server Products, Workstation Products and Application Products Tabs in attached Excel Sheet, to prioritize patch and patch management process for critical IT assets

## WORKAROUND

If you’re unable to upgrade at this time, you can use this script to temporarily protect SolarWinds Orion environment against the SUPERNOVA malware, and abusive attacks.

## INTRODUCTION

Microsoft released security patches for 83 vulnerabilities in various Microsoft products such as Windows Workstations & Servers, MS SQL, SharePoint and Office, which would allow unauthenticated remote attacker to execute malicious code in the context of user account.

And also, Microsoft released security patches for very critical vulnerabilities (CVE-2021-1647, CVE-2021-1648, CVE-2021-1678, CVE-2021-1674, CVE-2021-1669 and CVE-2021-1695) in Microsoft Windows Workstation and Server products, and CVE-2021-1707 in Microsoft SharePoint Server that are more likely to be exploited in targeted malware or ransomware attacks and hacking campaigns.
IMPORTANT

## IMPORTANT

Microsoft Windows 10 1903 Pro, Pro Education, Pro for Workstations, Enterprise, and IoT Enterprise, has reached end of service on December 8th, 2020.

Microsoft Windows 10 1803 Enterprise, IoT Enterprise, and education users get an extra year of servicing, with their end of support being May 11th, 2021.

Microsoft Windows 10 1803 Pro, Pro for Workstation, and IoT Core has reached end of support on November 12th, 2019, as well as Microsoft Windows 7 has reached end of support on January 14th, 2020, which means they will no longer receive security updates and will be vulnerable to any new security threats that are discovered. We recommend upgrading to latest supported versions of Microsoft Windows OS

## AFFECTED PRODUCTS

- Microsoft Windows Workstation and Server products.
- Microsoft Visual Studio, MS SQL, and SharePoint Servers products.
- Microsoft Edge, and Office products

## READ

- January 2021 Security Updates
- Microsoft January 2021 Patch Tuesday fixes 83 flaws, 1 zero-day

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

# The xHunt campaign that continued to target Government, Defense, and Privately held organizations in the Middle East

Severity: High

Date: January 13, 2021

## IP ADDRESS

142.11.211.79
91.92.109.59
192.119.110.194
192.255.166.158
77.243.191.20
185.220.70.144
193.176.86.134
82.102.21.219
89.26.241.70
23.92.127.18
196.52.84.35
196.52.84.52
185.220.70.139
185.230.127.233
185.230.127.239
193.176.86.170
212.102.52.134
212.102.35.102
196.52.84.30
185.230.127.238
89.238.139.52
195.181.170.242
89.238.137.37
92.223.89.137
85.203.46.99
185.246.208.197
92.223.89.134
92.223.89.136
195.181.170.243
84.17.55.68
46.246.3.254
46.246.3.253

## IP ADDRESS

POQSBWBKAHZLRWNZFVPG
RCWIWFL0MCDGZKGO0A
NCHOOJMDGUYAOWZVXJQDG
ITKVJLNUKULNR0PBAWQ
IJFHUUAID0FGS9YQEMHCG
IJAJGSWXUWVDVMMUHQQ
IIARASUWFCYUBMI0NA
QAFCNW0FN0ENKWGZPEPVW
HKPBNWFKIYLNWUGAHJA
OWITUR9UOKSZPXDKFBW
YEHIZAWKCLYFMDS9Q
VOICHQVTFKIDXTCAKA
INAYIKTWB0WGQOW0SRHWAQ

## REMEDIATION

Ensure Microsoft Windows Servers and Workstations are updated with latest security patches.
2. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with 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 allows 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 unusual amount of data transmission, etc.
5. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor 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 VPN tunnel.
7. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.
8. Strictly ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are not left open on 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 tunnel between VPN clients and 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 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 out-of-band network onto the server with limited or no internet access.
14. Kindly Block IP Address, Domain, and Client ID, on the perimeter security devices.

## DOMAINS

backendloop.online
bestmg.info
windowsmicrosofte.online

## READ

- xHunt Campaign: New BumbleBee Webshell and SSH Tunnels Used for Lateral Movement

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

# North Korea-based APT37 Threat Actors that were found targeting the government organizations in South Korea with the RokRat malware

Severity: High

Date: January 07, 2021

## IP ADDRESS

74.120.9.233

## DOMAIN

deman1.icu
hotsoft.icu
uplearn.top
lidarcc.icu
sharepoint-web.com

## URLS

http<://>bit.ly/2Np1enh

https<://>drive.google.com/uc?export=download&id=1XQwiYeCCV0C-SsP7iPwD5FGSHit5yysv

https<://>doc-08-9odocs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/bgag60bttqvb3n1e8err6c0nu0e66fat/1610023275000/00614111482142402963/*/1XQwiYeCCV0CSsP7iPwD5FGSHit5yysv?e=download

## REMEDIATION

Ensure Microsoft Windows Servers and Workstations, are updated with latest security patches.
2. 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.
3. Ensure network segments that allows 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 unusual amount of data transmission, etc.
4. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor authentication is enabled on all Business Email Accounts.
5. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
6. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.
7. Strictly ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are not left open on Internet or DMZ facing side.
8. Please ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389, are only accessible through VPN tunnel between VPN clients and Organization's Resources.
9. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
10. Ensure to monitor for excessive LDAP queries within 5 minutes from particular system, via SIEM solution.
11. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.
12. 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.
13. Kindly Block IP Address, Domain, and URLs, on the perimeter security devices.
14. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor

## READ

- Retrohunting APT37: North Korean APT used VBA self decode technique to inject RokRat

## HASH (SHA-256)

| Hashes | DETECTED BY ANTIVIRUS | | | | |
|---|---|---|---|---|---|
| | Symantec | TrendMicro | McAfee | Quick Heal | Microsoft |
| 3C59AD7C4426E8396369F084C35A2BD3F0CAA3BA1D1A917941535072 10A77C90 | Yes | Yes | No | Yes | Yes |
| E2CA463A25D532A9AF6E9105F073C2E3CC4695ECBB9CE1FC35CBC8F5CC89AF94 | No | No | No | No | No |
| 676AE680967410E0F245DF0B6163005D8799C84E2F8F87BAD6B5E30295554E08 | Yes | Yes | Yes | Yes | Yes |
| A42844FC9CB7F80CA49726B3589700FA47BDACF787202D0461C753E7C73CFD2A | Yes | No | Yes | No | Yes |
| 2A253C2AA1DB3F809C86F410E4BD21F680B7235D951567F24D614D8E4D041576 | Yes | Yes | Yes | Yes | Yes |

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

# An Authentication Bypass vulnerability (CVE-2020-10148) in Solarwinds Orion which allowed remote command execution from unauthenticated remote attackers

Severity: Critical

Date: December 29, 2020

## IMPACT

This vulnerability poses a severe risk of
unauthorized access, security breach, data breach, supply-chain attack, impact customers, impact business operations, impact business brand and reputation of an organization.

## REMEDIATION

1. Upgrade Solarwinds Orion, to version 2020.2.1HF2 or higher
2. Upgrade Solarwinds Orion, to version 2019.4HF6 or higher
3. Upgrade Solarwinds Orion, to version 2019.2 SUPERNOVA Patch or higher
4. Upgrade Solarwinds Orion, to version 2018.4 SUPERNOVA Patch or higher
5. Upgrade Solarwinds Orion, to version 2018.2 SUPERNOVA Patch or higher.

## WORKAROUND

If you’re unable to upgrade at this time, you can use this script to temporarily protect SolarWinds Orion environment against the SUPERNOVA malware, and abusive attacks.

## INTRODUCTION

An Authentication Bypass vulnerability (CVE-2020-10148) lies within API module of SolarWinds Orion, which allow unauthenticated remote attackers to gain unauthorized access on SolarWinds Orion, execute remote commands, and perform supply-chain attack for wide distribution of malware.

To exploit this vulnerability, the unauthenticated remote attacker needs to craft API query by including specific parameters such as WebResource.adx, ScriptResource.adx, i18n.ashx or Skipi18n in the Request.PathInfo portion of a URI request and send it towards the
affected versions of SolarWinds Orion server. As a result, the SolarWinds Orion server will set the SkipAuthorization flag, to allow the processing of API requests without requiring authentication. And any further access to functional APIs will allow unauthenticated remote attackers to execute remote code or command on affected versions of SolarWinds Orion server.

This vulnerability poses a severe risk of unauthorized access, security breach, data breach, supply-chain attack, impact customers, impact business operations, impact business brand and reputation of an organization

## AFFECTED PRODUCTS

- Solarwinds Orion versions prior to 2020.2.1HF2
- Solarwinds Orion versions prior to 2019.4HF6
- Solarwinds Orion versions prior to 2019.2 SUPERNOVA Patch
- Solarwinds Orion versions prior to 2018.4 SUPERNOVA Patch
- •olarwinds Orion versions prior to 2018.2 SUPERNOVA Patch

## READ

- SolarWinds Orion API authentication bypass allows remote command execution
- SolarWinds Security Advisory
- New Zero-Day, Malware Indicate Second Group May Have Targeted SolarWinds
- Rule for CVE-2020-10148 - SolarWinds Orion
- POC for CVE-2020-10148 - SolarWinds Orion

NETWORK INTELLIGENCE
Global cybersecurity provider

# Security Patch Advisory

4th January 2021 – 10th January 2021 | TRAC-ID: NII21.01.0.2

| Severity Matrix | | | |
|---|---|---|---|
| L | M | H | C |
| Low | Medium | High | Critical |

## UBUNTU

| | TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|---|
| January 08, 2021 | Ubuntu Linux | USN-4687-1: Firefox vulnerability | ▪ Ubuntu 20.10<br>▪ Ubuntu 20.04 LTS<br>▪ Ubuntu 18.04 LTS<br>▪ Ubuntu 16.04 LTS | Kindly update to fixed version |
| January 07, 2021 | Ubuntu Linux | USN-4686-1: Ghostscript vulnerabilities | ▪ Ubuntu 18.04 LTS<br>▪ Ubuntu 16.04 LTS | Kindly update to fixed version |
| January 07, 2021 | Ubuntu Linux | USN-4685-1: OpenJPEG vulnerabilities | ▪ Ubuntu 20.10<br>▪ Ubuntu 20.04 LTS | Kindly update to fixed version |

## REDHAT

| | TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|---|
| January 05, 2021 | Red Hat Enterprise Linux | RHSA-2021:0024 | ▪ Red Hat Enterprise Linux Server 7 x86_64<br>▪ Red Hat Enterprise Linux Workstation 7 x86_64<br>▪ Red Hat Enterprise Linux Desktop 7 x86_64 | Kindly update to fixed version |
| January 05, 2021 | Red Hat Enterprise Linux | RHSA-2021:0019 | ▪ Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.7 x86_64<br>▪ Red Hat Enterprise Linux Server - AUS 7.7 x86_64<br>▪ Red Hat Enterprise Linux EUS Compute Node 7.7 x86_64<br>▪ Red Hat Enterprise Linux Server - TUS 7.7 x86_64 | Kindly update to fixed version |

NETWORK INTELLIGENCE
Global cybersecurity provider

# Security Patch Advisory

4th January 2021 – 10th January 2021 | TRAC-ID: NII21.01.0.2

| | | | | |
|---|---|---|---|---|
| January 04, 2021 | **Red Hat Enterprise Linux** | RHSA-2021:0004 | ▪ Red Hat Enterprise Linux for Real Time 8 x86_64<br>▪ Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 | Kindly update to fixed version |
| January 04, 2021 | **Red Hat Enterprise Linux** | RHSA-2021:0003 | ▪ Red Hat Enterprise Linux for x86_64 8 x86_64<br>▪ Red Hat Enterprise Linux for ARM 64 8 aarch64 | Kindly update to fixed version |

## IBM

| | TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|---|
| January 08, 2021 | **IBM MQ Appliance** | IBM MQ Appliance is affected by a denial of service vulnerability (CVE-2020-4869) | ▪ IBM MQ Appliance 9.2 CD<br>▪ IBM MQ Appliance 9.2 LTS | Kindly update to fixed version |
| January 07, 2021 | **IBM API Connect** | IBM API Connect is vulnerable to denial of service (DoS) via PHP (CVE-2020-7068) | ▪ IBM API Connect V10.0.0<br>▪ IBM API Connect V2018.4.1.0 - 2018.4.1.12<br>▪ IBM API Connect V5.0.0.0 - 5.0.8.9 | Kindly update to fixed version |
| January 07, 2021 | **IBM API Connect** | IBM API Connect V5 is vulnerable to cross-site scripting in jQuery (CVE-2015-9251) | ▪ IBM API Connect V5.0.0.0 - 5.0.8.10 | Kindly update to fixed version |