Writeup:

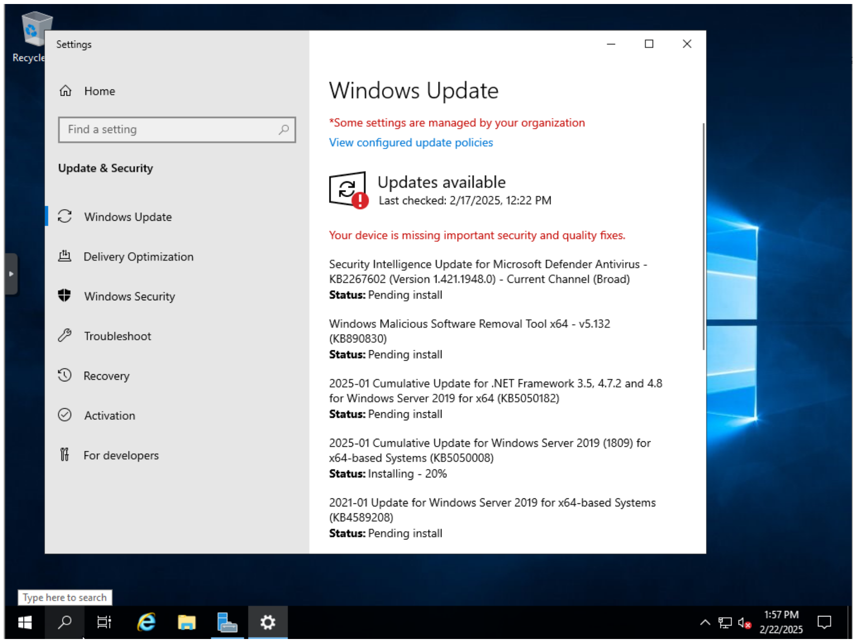
For non-patching vulnerabilities, my approach would begin with thorough research. I would review vendor advisories, security bulletins, technical documentation, and reputable vulnerability databases (such as NVD) to understand the specifics, potential exploit paths, and real-world impact of each vulnerability. I'd also engage with industry forums and peer-reviewed security reports to validate findings and gather additional remediation insights. Based on this research, I would implement the following compensating controls:

- **Network Segmentation:** Isolate unsupported systems using dedicated VLANs and strict firewall rules to restrict exposure to only trusted segments.
- **Access Controls & IAM:** Harden authentication by disabling high-risk accounts (e.g., Guest), removing them from privileged groups, and enforcing multi-factor authentication using solutions like YubiKey.
- **Enhanced Monitoring:** Deploy host-based IDS/IPS and centralize log collection to detect and alert on anomalous behavior in real time.
- **Application-Specific Restrictions:** For systems (e.g., an outdated Splunk instance) that can't be patched immediately, restrict network access and service exposure until a full upgrade is feasible.
- **Regular Risk Assessments:** Schedule continuous vulnerability scans with tools like Nessus and CrowdStrike to validate the effectiveness of these controls and refine configurations as needed.

This comprehensive strategy minimizes risk by addressing residual vulnerabilities with targeted technical controls while ensuring that all research and remediation steps are well documented for audit and future remediation purposes.

172.16.1.3 – DNS Server (Updated OS)

Check for any window updates



Windows Update

*Some settings are managed by your organization

View configured update policies

Updates available

Last checked: 2/17/2025, 12:22 PM

Your device is missing important security and quality fixes.

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1948.0) - Current Channel (Broad)
Status: Pending install

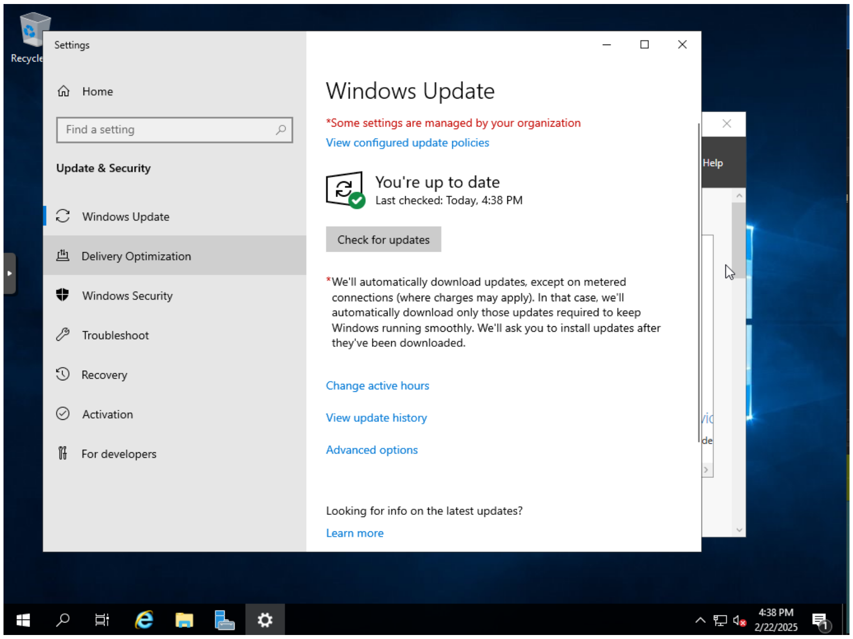
Windows Malicious Software Removal Tool x64 - v5.132 (KB890830)
Status: Pending install

2025-01 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5050182)
Status: Pending install

2025-01 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems (KB5050008)
Status: Installing - 20%

2021-01 Update for Windows Server 2019 for x64-based Systems (KB4589208)
Status: Pending install

Update windows – restart computer – ensure all updates were installed



Windows Update

*Some settings are managed by your organization

View configured update policies

You're up to date

Last checked: Today, 4:38 PM

*We'll automatically download updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly. We'll ask you to install updates after they've been downloaded.

Change active hours

View update history

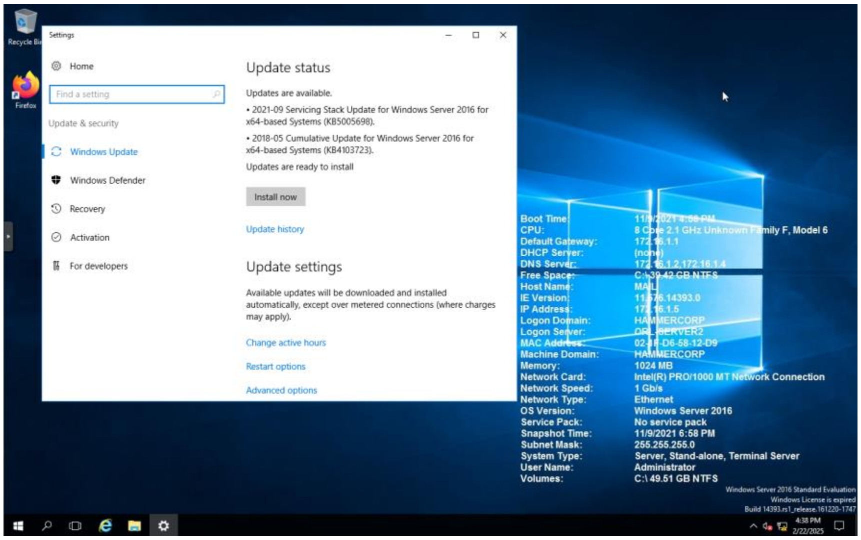
Advanced options

Looking for info on the latest updates?

Learn more

172.16.1.5 – Mail Server (Fixed SWEET32)

Ensure all operating system updates are installed



Settings

Update status

Updates are available.

- 2021-09 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5005698).
- 2018-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4103723).

Updates are ready to install

Update settings

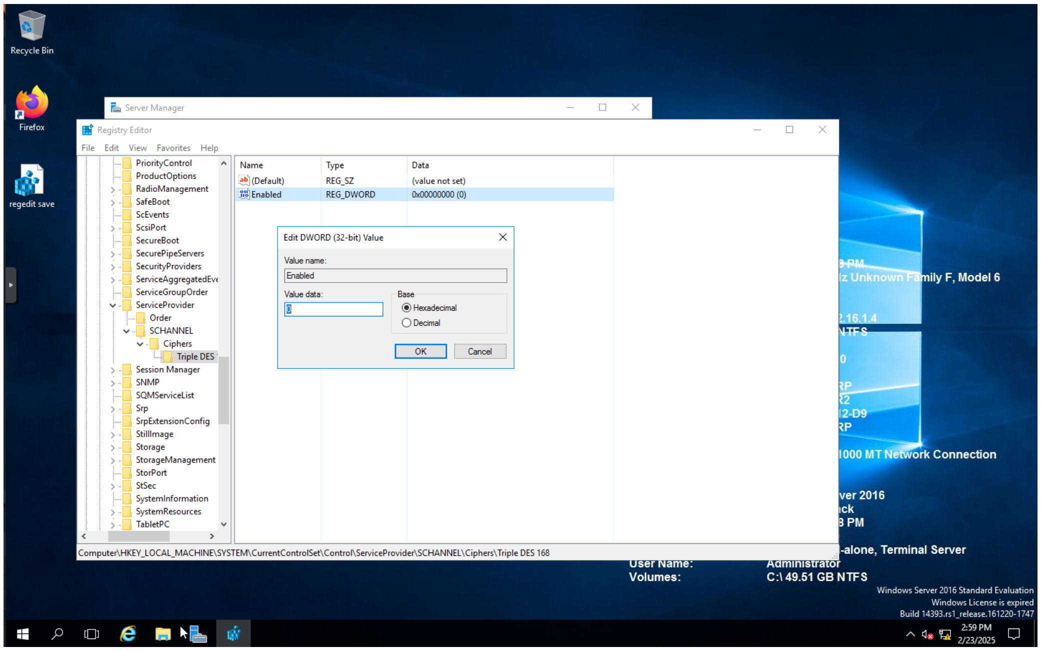
Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

```
Boot Time:        11/9/2021 4:58 PM
CPU:              8 Core 2.1 GHz Unknown Family F, Model 6
Default Gateway:  172.16.1.1
DHCP Server:      (none)
DNS Server:       172.16.1.2,172.16.1.4
Free Space:       C:\ 39.42 GB NTFS
Host Name:        MAIL
IE Version:       11.576.14393.0
IP Address:       172.16.1.5
Logon Domain:     HAMMERCORP
Logon Server:     ORL-SERVER2
MAC Address:      02-1F-D6-58-12-D9
Machine Domain:   HAMMERCORP
Memory:           1024 MB
Network Card:     Intel(R) PRO/1000 MT Network Connection
Network Speed:    1 Gb/s
Network Type:     Ethernet
OS Version:       Windows Server 2016
Service Pack:     No service pack
Snapshot Time:    11/9/2021 6:58 PM
Subnet Mask:      255.255.255.0
System Type:      Server, Stand-alone, Terminal Server
User Name:        Administrator
Volumes:          C:\ 49.51 GB NTFS
```

Windows Server 2016 Standard Evaluation
Windows License is expired
Build 14393.rs1_release.161220-1747

4:38 PM
2/22/2025

Open registry editor and find service provider – create SCHANNEL, ciphers, Triple DES – create a new DWORD value and give it the value of 0



Registry Editor

Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000000 (0)

Edit DWORD (32-bit) Value

Value name: Enabled

Value data: 0

Base: ● Hexadecimal ○ Decimal

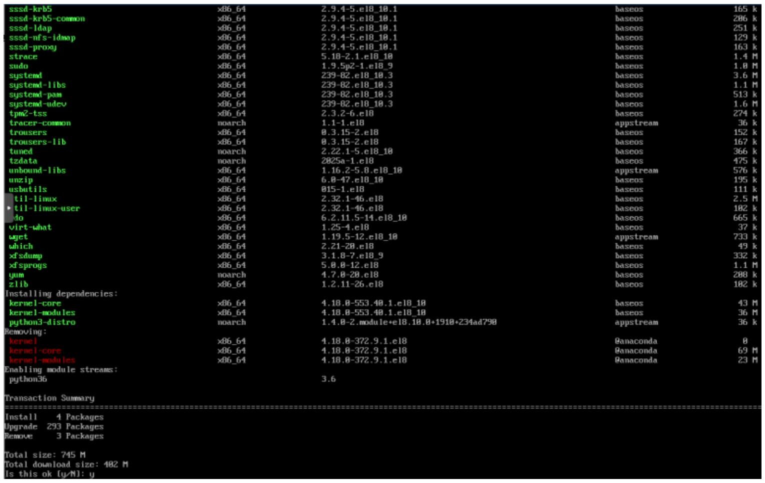
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceProvider\SCHANNEL\Ciphers\Triple DES 168

Windows Server 2016 Standard Evaluation
Windows License is expired
Build 14393.rs1_release.161220-1747

2:59 PM
2/23/2025

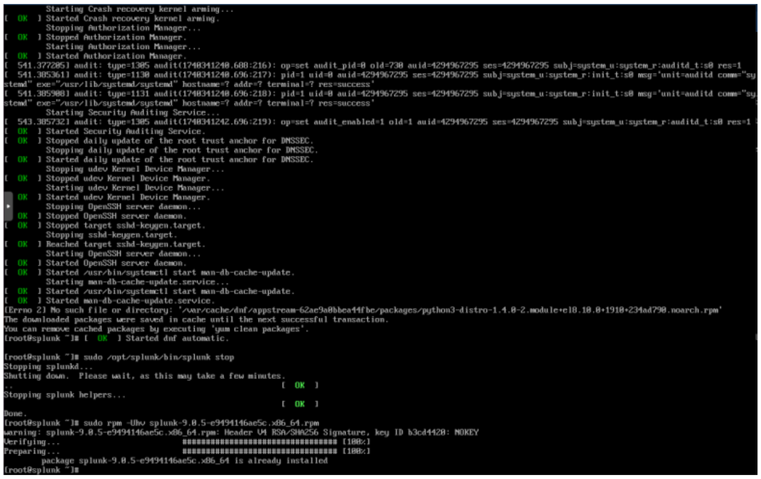
172.16.1.6 – Splunk (Updated OS & Splunk) (Splunk still needs newer version)

Sudo yum update – ensure OS is updated



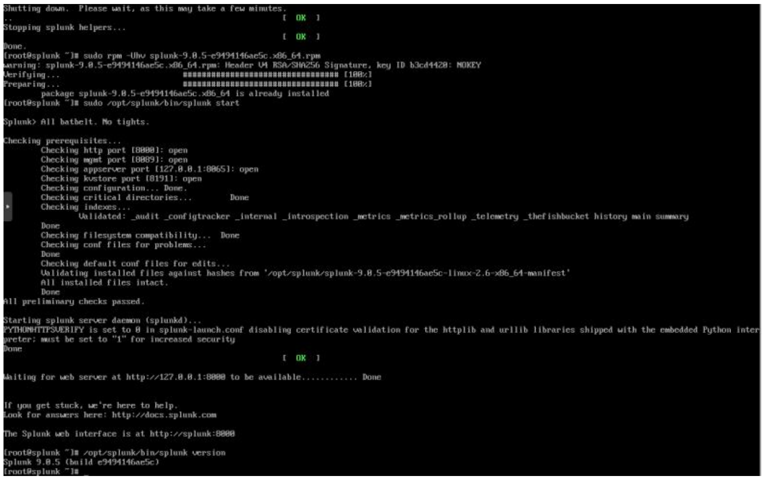
```
 sssd-krb5                  x86_64        2.9.4-5.el8_10.1                        baseos          165 k
 sssd-krb5-common           x86_64        2.9.4-5.el8_10.1                        baseos          206 k
 sssd-ldap                  x86_64        2.9.4-5.el8_10.1                        baseos          251 k
 sssd-nfs-idmap             x86_64        2.9.4-5.el8_10.1                        baseos          129 k
 sssd-proxy                 x86_64        2.9.4-5.el8_10.1                        baseos          163 k
 strace                     x86_64        5.18-2.1.el8_10                         baseos          1.4 M
 sudo                       x86_64        1.9.5p2-1.el8_9                         baseos          1.0 M
 systemd                    x86_64        239-82.el8_10.3                         baseos          3.6 M
 systemd-libs               x86_64        239-82.el8_10.3                         baseos          1.1 M
 systemd-pam                x86_64        239-82.el8_10.3                         baseos          513 k
 systemd-udev               x86_64        239-82.el8_10.3                         baseos          1.6 M
 tpm2-tss                   x86_64        2.3.2-6.el8                             baseos          274 k
 tracer-common              noarch        1.1-1.el8                               appstream        36 k
 trousers                   x86_64        0.3.15-2.el8                            baseos          152 k
 trousers-lib               x86_64        0.3.15-2.el8                            baseos          167 k
 tuned                      noarch        2.22.1-5.el8_10                         baseos          366 k
 tzdata                     noarch        2025a-1.el8                             baseos          475 k
 unbound-libs               x86_64        1.16.2-5.8.el8_10                       appstream       576 k
 unzip                      x86_64        6.0-47.el8_10                           baseos          195 k
 usbutils                   x86_64        015-1.el8                               baseos          111 k
 til-linux                  x86_64        2.32.1-46.el8                           baseos          2.5 M
 til-linux-user             x86_64        2.32.1-46.el8                           baseos          102 k
 do                         x86_64        6.2.11.5-14.el8_10                      baseos          665 k
 virt-what                  x86_64        1.25-4.el8                              baseos           37 k
 wget                       x86_64        1.19.5-12.el8_10                        appstream       733 k
 which                      x86_64        2.21-20.el8                             baseos           49 k
 xfsdump                    x86_64        3.1.8-7.el8_9                           baseos          332 k
 xfsprogs                   x86_64        5.0.0-12.el8                            baseos          1.1 M
 yum                        noarch        4.7.0-20.el8                            baseos          208 k
 zlib                       x86_64        1.2.11-26.el8                           baseos          102 k
Installing dependencies:
 kernel-core                x86_64        4.18.0-553.40.1.el8_10                  baseos           43 M
 kernel-modules             x86_64        4.18.0-553.40.1.el8_10                  baseos           36 M
 python3-distro             noarch        1.4.0-2.module+el8.10.0+1910+234ad790   appstream        36 k
Removing:
 kernel                     x86_64        4.18.0-372.9.1.el8                      @anaconda         0
 kernel-core                x86_64        4.18.0-372.9.1.el8                      @anaconda        69 M
 kernel-modules             x86_64        4.18.0-372.9.1.el8                      @anaconda        23 M
Enabling module streams:
 python36                                 3.6

Transaction Summary
=======================================================================================================
Install    4 Packages
Upgrade  293 Packages
Remove     3 Packages

Total size: 745 M
Total download size: 402 M
Is this ok [y/N]: y
```

Stop splunk service and install new verison



```
         Starting Crash recovery kernel arming...
[  OK  ] Started Crash recovery kernel arming.
         Stopping Authorization Manager...
[  OK  ] Stopped Authorization Manager.
         Starting Authorization Manager...
[  OK  ] Started Authorization Manager.
[  541.377205] audit: type=1305 audit(1740341240.680:216): op=set audit_pid=0 old=730 auid=4294967295 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=1
[  541.385361] audit: type=1130 audit(1740341240.696:217): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="sy
stemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
[  541.385908] audit: type=1131 audit(1740341240.696:218): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="sy
stemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
         Starting Security Auditing Service...
[  543.385732] audit: type=1305 audit(1740341242.696:219): op=set audit_enabled=1 old=1 auid=4294967295 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=1
[  OK  ] Started Security Auditing Service.
[  OK  ] Stopped daily update of the root trust anchor for DNSSEC.
         Stopping daily update of the root trust anchor for DNSSEC.
[  OK  ] Started daily update of the root trust anchor for DNSSEC.
         Stopping udev Kernel Device Manager...
[  OK  ] Stopped udev Kernel Device Manager.
         Starting udev Kernel Device Manager...
   OK  ] Started udev Kernel Device Manager.
         Stopping OpenSSH server daemon...
   OK  ] Stopped OpenSSH server daemon.
[  OK  ] Stopped target sshd-keygen.target.
         Stopping sshd-keygen.target.
[  OK  ] Reached target sshd-keygen.target.
         Starting OpenSSH server daemon...
[  OK  ] Started OpenSSH server daemon.
[  OK  ] Started /usr/bin/systemctl start man-db-cache-update.
         Starting man-db-cache-update.service...
[  OK  ] Started /usr/bin/systemctl start man-db-cache-update.
[  OK  ] Started man-db-cache-update.service.
[Errno 2] No such file or directory: '/var/cache/dnf/appstream-62ae9a0bbea44fbc/packages/python3-distro-1.4.0-2.module+el8.10.0+1910+234ad790.noarch.rpm'
The downloaded packages were saved in cache until the next successful transaction.
You can remove cached packages by executing 'yum clean packages'.
[root@splunk ~]# [  OK  ] Started dnf automatic.

[root@splunk ~]# sudo /opt/splunk/bin/splunk stop
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
..                                                         [  OK  ]
Stopping splunk helpers...
                                                           [  OK  ]
Done.
[root@splunk ~]# sudo rpm -Uhv splunk-9.0.5-e9494146ae5c.x86_64.rpm
warning: splunk-9.0.5-e9494146ae5c.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID b3cd4420: NOKEY
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
        package splunk-9.0.5-e9494146ae5c.x86_64 is already installed
[root@splunk ~]#
```

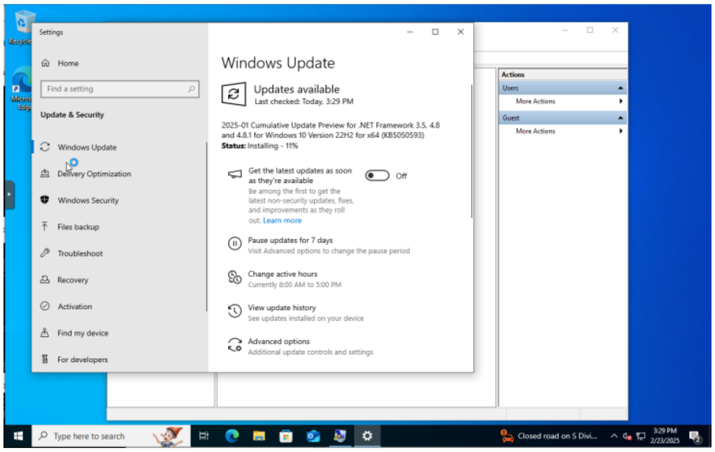
Start splunk service & check version



```
Shutting down.  Please wait, as this may take a few minutes.
..                                                         [  OK  ]
Stopping splunk helpers...
                                                           [  OK  ]
Done.
[root@splunk ~]# sudo rpm -Uhv splunk-9.0.5-e9494146ae5c.x86_64.rpm
warning: splunk-9.0.5-e9494146ae5c.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID b3cd4420: NOKEY
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
        package splunk-9.0.5-e9494146ae5c.x86_64 is already installed
[root@splunk ~]# sudo /opt/splunk/bin/splunk start

Splunk> All batbelt. No tights.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _configtracker _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-9.0.5-e9494146ae5c-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python inter
preter; must be set to "1" for increased security
Done
                                                           [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available............ Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk:8000

[root@splunk ~]# /opt/splunk/bin/splunk version
Splunk 9.0.5 (build e9494146ae5c)
[root@splunk ~]# _
```

172.16.1.100 – ORLWorkstation (Patched SWEET32 & Guest Groups)

Check for any updates



Windows Update

Updates available
Last checked: Today, 3:29 PM

2025-01 Cumulative Update Preview for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5050593)
Status: Installing - 11%

Get the latest updates as soon as they're available — Off
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. Learn more

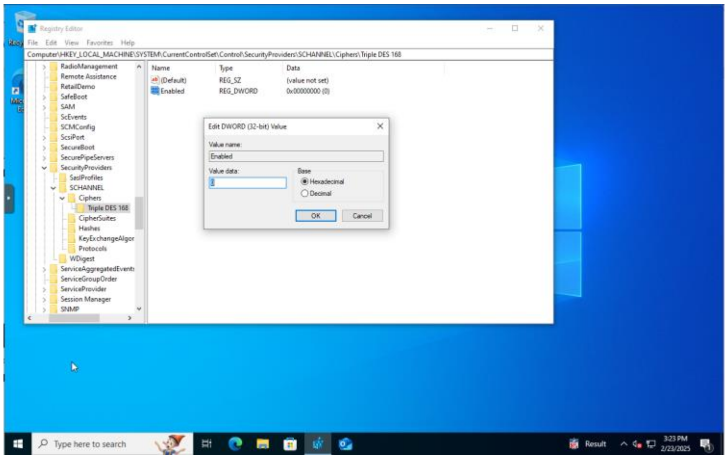
Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 8:00 AM to 5:00 PM

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Disable the vulnerable cipher through SCHANNEL



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168

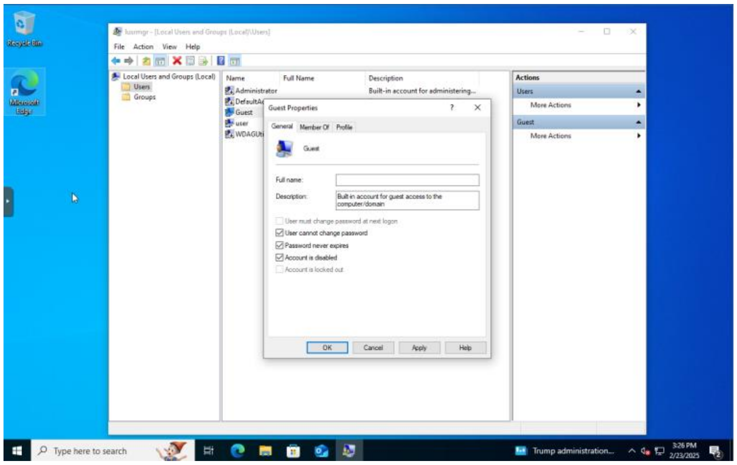
Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000000 (0)

Edit DWORD (32-bit) Value

Value name: Enabled
Value data: 0
Base: ● Hexadecimal ○ Decimal

OK Cancel

Go to – lusrmgr.msc – view guest account – Disable it as its not needed (or redefine groups)



Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultA...		
Guest		
user		
WDAGUti...		

Guest Properties

General | Member Of | Profile

Guest

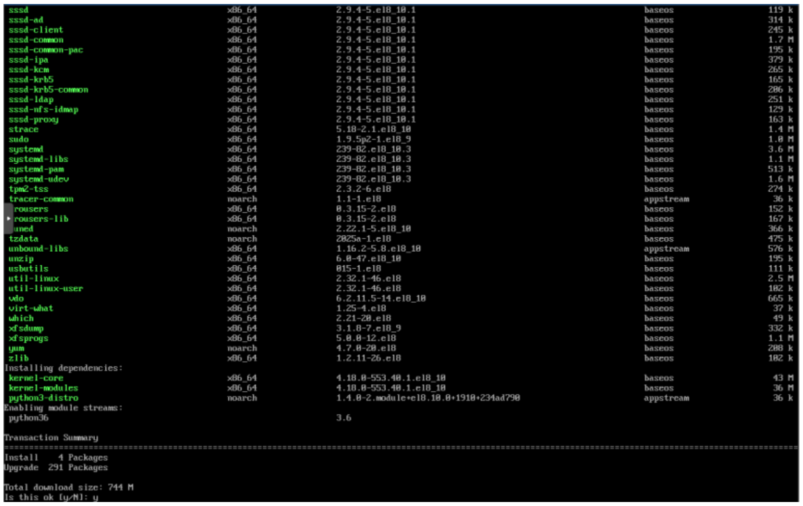
Full name:
Description: Built-in account for guest access to the computer/domain

□ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☑ Account is disabled
□ Account is locked out

OK Cancel Apply Help

172.16.1.105 – Nessus Server (Patched by updated OS)

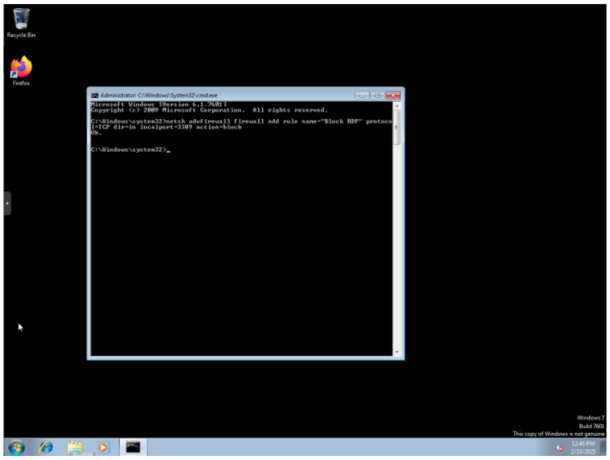
Sudo Yum Update



```
 sssd                         x86_64      2.9.4-5.el8_10.1                             baseos        119 k
 sssd-ad                      x86_64      2.9.4-5.el8_10.1                             baseos        314 k
 sssd-client                  x86_64      2.9.4-5.el8_10.1                             baseos        245 k
 sssd-common                  x86_64      2.9.4-5.el8_10.1                             baseos        1.7 M
 sssd-common-pac              x86_64      2.9.4-5.el8_10.1                             baseos        195 k
 sssd-ipa                     x86_64      2.9.4-5.el8_10.1                             baseos        379 k
 sssd-kcm                     x86_64      2.9.4-5.el8_10.1                             baseos        265 k
 sssd-krb5                    x86_64      2.9.4-5.el8_10.1                             baseos        165 k
 sssd-krb5-common             x86_64      2.9.4-5.el8_10.1                             baseos        206 k
 sssd-ldap                    x86_64      2.9.4-5.el8_10.1                             baseos        251 k
 sssd-nfs-idmap               x86_64      2.9.4-5.el8_10.1                             baseos        129 k
 sssd-proxy                   x86_64      2.9.4-5.el8_10.1                             baseos        163 k
 strace                       x86_64      5.18-2.1.el8_10                              baseos        1.4 M
 sudo                         x86_64      1.9.5p2-1.el8_9                              baseos        1.0 M
 systemd                      x86_64      239-82.el8_10.3                              baseos        3.6 M
 systemd-libs                 x86_64      239-82.el8_10.3                              baseos        1.1 M
 systemd-pam                  x86_64      239-82.el8_10.3                              baseos        513 k
 systemd-udev                 x86_64      239-82.el8_10.3                              baseos        1.6 M
 tpm2-tss                     x86_64      2.3.2-6.el8                                  baseos        274 k
 tracer-common                noarch      1.1-1.el8                                    appstream      36 k
  rousers                     x86_64      0.3.15-2.el8                                 baseos        152 k
  rousers-lib                 x86_64      0.3.15-2.el8                                 baseos        167 k
  uned                        noarch      2.22.1-5.el8_10                              baseos        366 k
 tzdata                       noarch      2025a-1.el8                                  baseos        475 k
 unbound-libs                 x86_64      1.16.2-5.8.el8_10                            appstream     576 k
 unzip                        x86_64      6.0-47.el8_10                                baseos        195 k
 usbutils                     x86_64      015-1.el8                                    baseos        111 k
 util-linux                   x86_64      2.32.1-46.el8                                baseos        2.5 M
 util-linux-user              x86_64      2.32.1-46.el8                                baseos        102 k
 vdo                          x86_64      6.2.11.5-14.el8_10                           baseos        665 k
 virt-what                    x86_64      1.25-4.el8                                   baseos         37 k
 which                        x86_64      2.21-20.el8                                  baseos         49 k
 xfsdump                      x86_64      3.1.8-7.el8_9                                baseos        332 k
 xfsprogs                     x86_64      5.0.0-12.el8                                 baseos        1.1 M
 yum                          noarch      4.7.0-20.el8                                 baseos        208 k
 zlib                         x86_64      1.2.11-26.el8                                baseos        102 k
Installing dependencies:
 kernel-core                  x86_64      4.18.0-553.40.1.el8_10                       baseos         43 M
 kernel-modules               x86_64      4.18.0-553.40.1.el8_10                       baseos         36 M
 python3-distro               noarch      1.4.0-2.module+el8.10.0+1910+234ad790        appstream      36 k
Enabling module streams:
 python36                                 3.6

Transaction Summary
==========================================================================================================
Install    4 Packages
Upgrade  291 Packages

Total download size: 744 M
Is this ok [y/N]: y
```

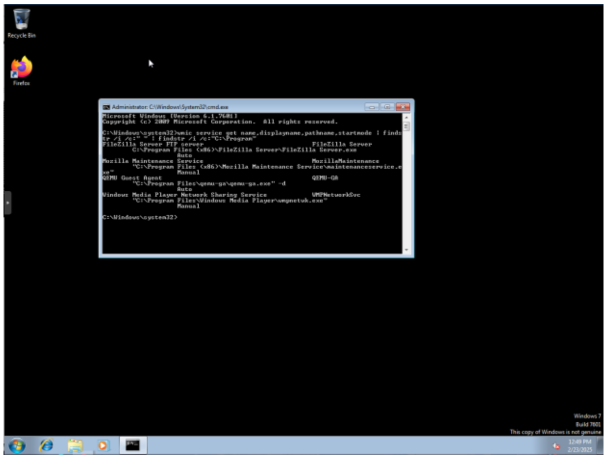
172.17.1.102 – SFOws (Fixed unquoted paths, SWEET32, & Guest account permissions) (OS is out of life and still needs to be updated or compensating controls put in place)

Add a new firewall rule to block RDP connections

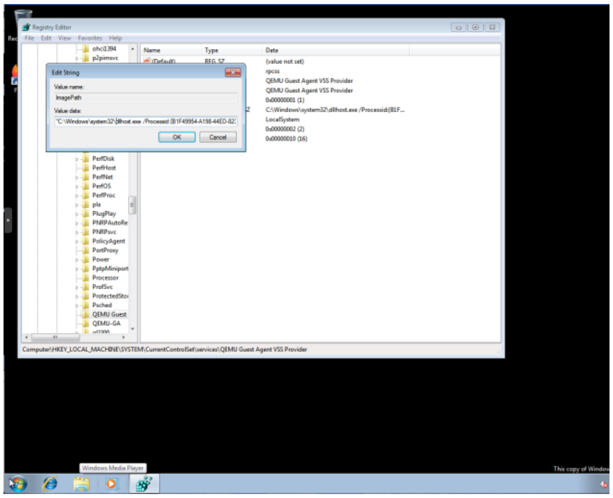

Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>netsh advfirewall firewall add rule name="Block RDP" protoco
l=TCP dir=in localport=3389 action=block
Ok.


C:\Windows\system32>_
```

Identify attack surface for unquoted path enumeration


Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>wmic service get name,displayname,pathname,startmode | finds
tr /i /v:" " | findstr /i /v:"C:\Program"
FileZilla Server FTP server                           FileZilla Server
        C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe
                    Auto
Mozilla Maintenance Service                           MozillaMaintenance
        "C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.e
xe"                 Manual
QEMU Guest Agent                                      QEMU-GA
        "C:\Program Files\qemu-ga\qemu-ga.exe" -d
                    Auto
Windows Media Player Network Sharing Service          WMPNetworkSvc
        "C:\Program Files\Windows Media Player\wmpnetwk.exe"
                    Manual

C:\Windows\system32>
```


Registry Editor

Edit String

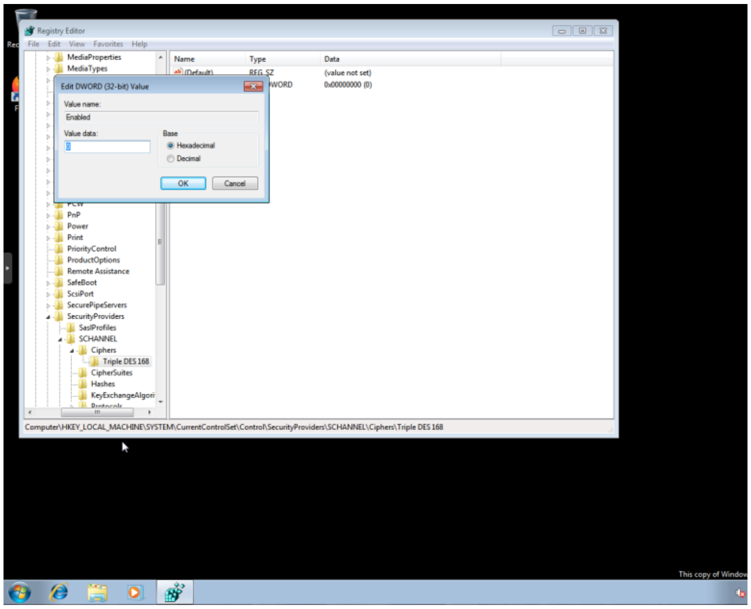
Value name:
ImagePath

Value data:
"C:\Windows\system32\dllhost.exe /Processid:{B1F49954-A198-44ED-82

Name	Type	Data
(Default)	REG_SZ	(value not set)
		rpcss
		QEMU Guest Agent VSS Provider
		QEMU Guest Agent VSS Provider
		0x00000001 (1)
	Z	C:\Windows\system32\dllhost.exe /Processid:{B1F...
		LocalSystem
		0x00000002 (2)
		0x00000010 (16)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\QEMU Guest Agent VSS Provider

Disable the vulnerable cipher through SCHANNEL



Name	Type	Data
(Default)	REG_SZ	(value not set)
	WORD	0x00000000 (0)

Edit DWORD (32-bit) Value

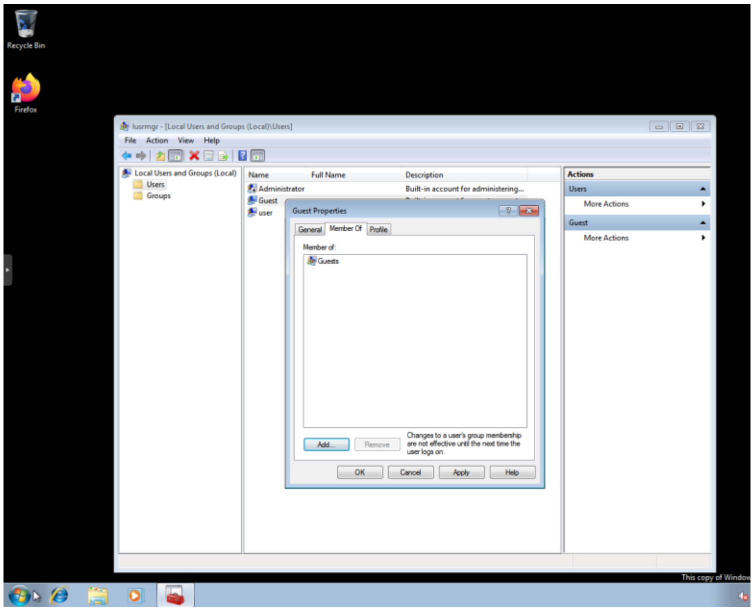
Value name: Enabled

Value data: 0

Base: ● Hexadecimal ○ Decimal

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168

Remove Guest accounts from other groups



Name	Full Name	Description
Administrator		Built-in account for administering...
Guest		
user		

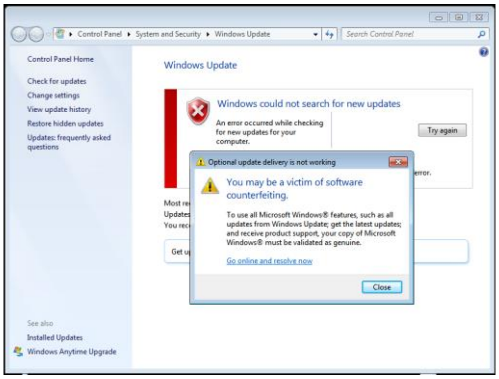
Guest Properties

Member of:

Guests

Changes to a user's group membership are not effective until the next time the user logs on.

Unsupported Windows OS (remote) – Unable to fix vulnerability due to using an outdated and pirated software



Windows Update

Windows could not search for new updates

An error occurred while checking for new updates for your computer.

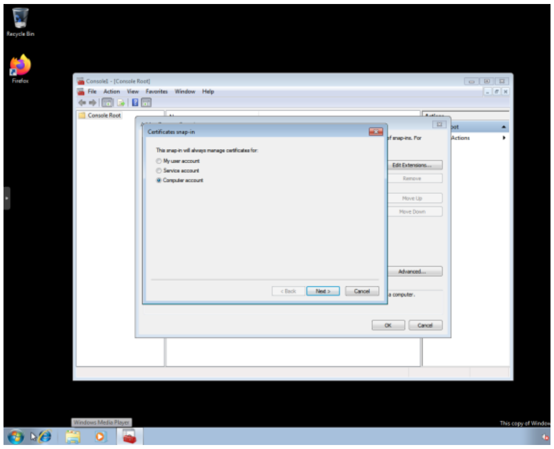
Optional update delivery is not working

You may be a victim of software counterfeiting.

To use all Microsoft Windows® features, such as all updates from Windows Update; get the latest updates; and receive product support, your copy of Microsoft Windows® must be validated as genuine.

Go online and resolve now

Unable to generate a new certificate – win r – MMC – certificates – personal – all task – request new certificate – followed wizard – couldn't complete



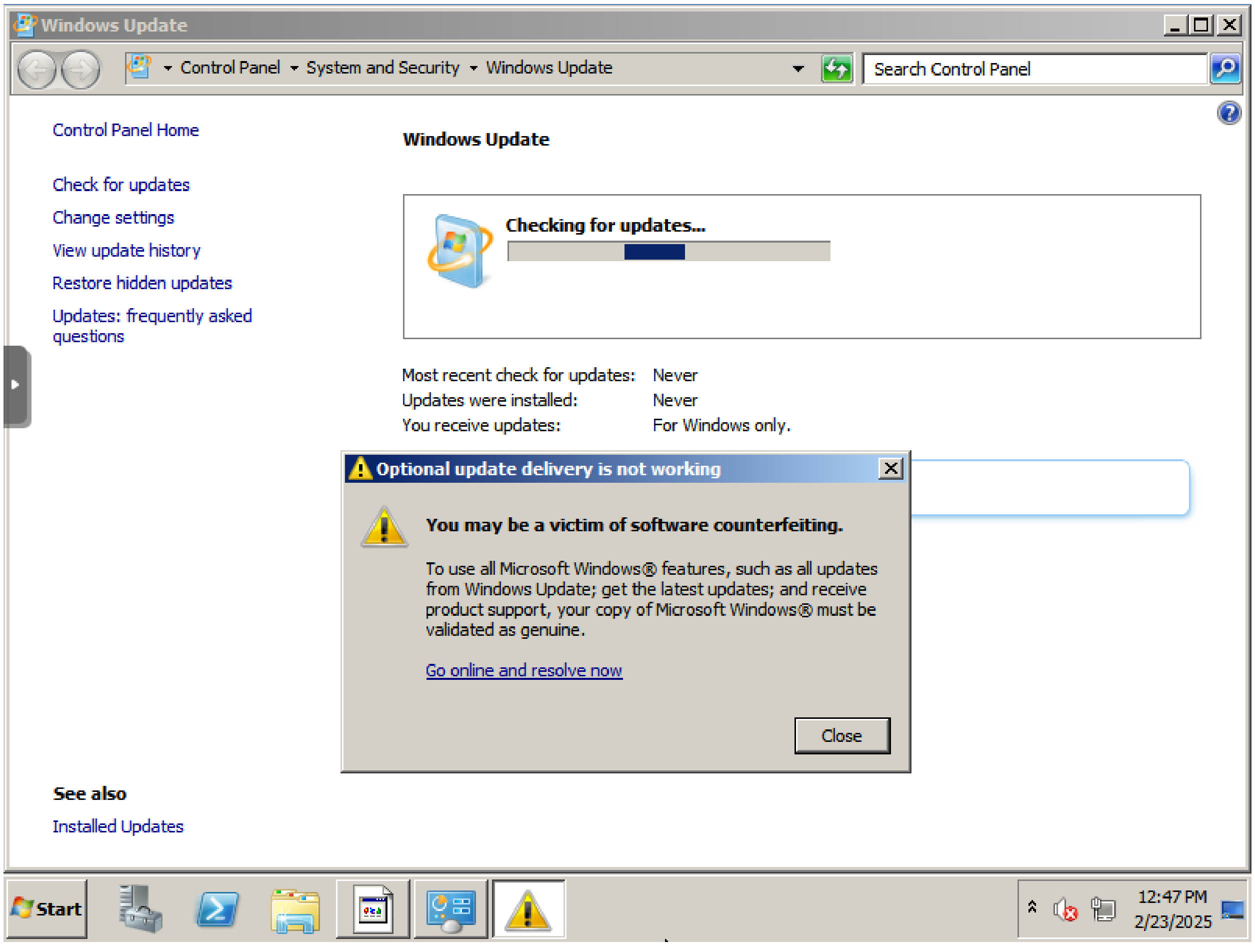
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

All Other Vulnerabilities are unable to be patched due to being on an unsupported operating system

172.17.1.2 – SFOServer (All vulnerabilities related to unsupported OS) (Add compensating controls or update OS if possible.)



Windows Update

Checking for updates...

Most recent check for updates: Never
Updates were installed: Never
You receive updates: For Windows only.

Optional update delivery is not working

You may be a victim of software counterfeiting.

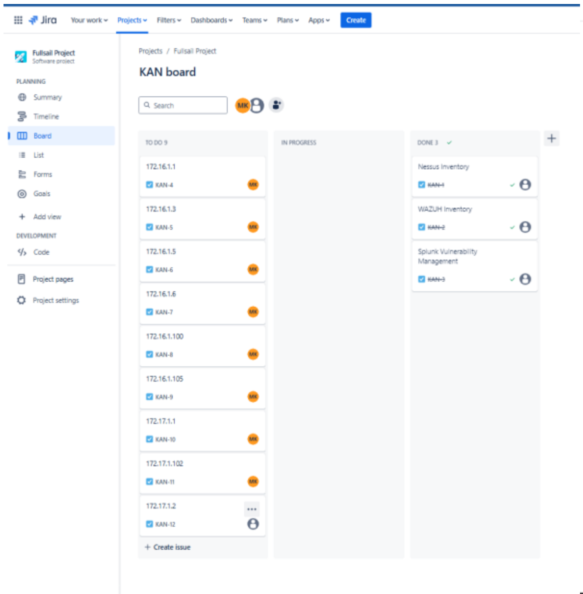
To use all Microsoft Windows® features, such as all updates from Windows Update; get the latest updates; and receive product support, your copy of Microsoft Windows® must be validated as genuine.

Go online and resolve now

Close

All vulnerabilities are due to being on an unsupported and outdated version of windows. The best action to take is to update the operating system. If that is not an option – Tightening network segmentation, restricting access via firewall, disabling unnecessary services, and consistent monitoring is vital to keep a strong security posture.

JIRA Ticketing:



Projects / Fullsail Project

KAN board

TO DO 9

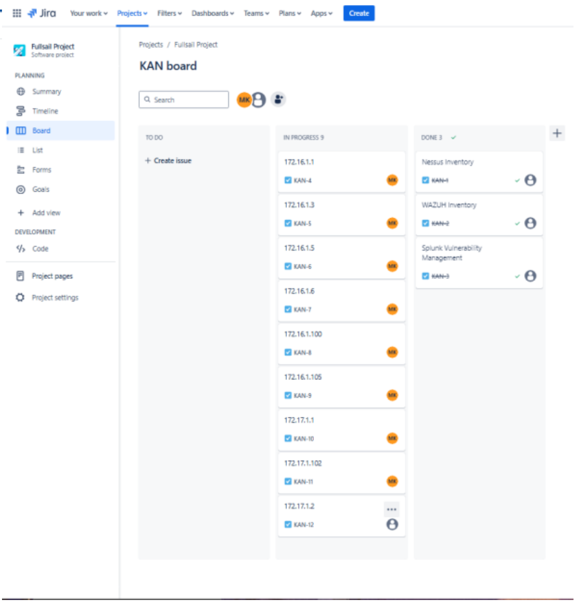
- 172.16.1.1 — KAN-4
- 172.16.1.3 — KAN-5
- 172.16.1.5 — KAN-6
- 172.16.1.6 — KAN-7
- 172.16.1.100 — KAN-8
- 172.16.1.105 — KAN-9
- 172.17.1.1 — KAN-10
- 172.17.1.102 — KAN-11
- 172.17.1.2 — KAN-12

+ Create issue

IN PROGRESS

DONE 3 ✓

- Nessus Inventory — ~~KAN-1~~
- WAZUH Inventory — ~~KAN-2~~
- Splunk Vulnerability Management — ~~KAN-3~~



Projects / Fullsail Project

KAN board

TO DO

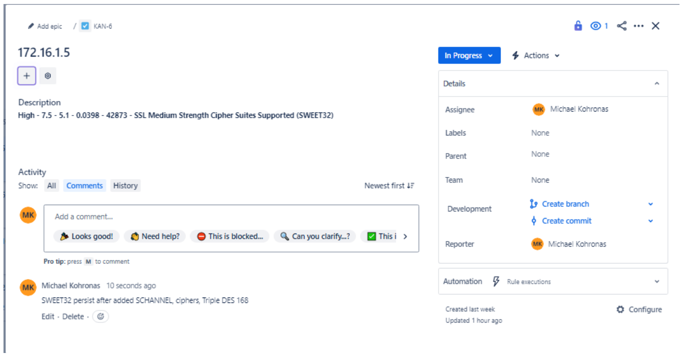
+ Create issue

IN PROGRESS 9

- 172.16.1.1 — KAN-4
- 172.16.1.3 — KAN-5
- 172.16.1.5 — KAN-6
- 172.16.1.6 — KAN-7
- 172.16.1.100 — KAN-8
- 172.16.1.105 — KAN-9
- 172.17.1.1 — KAN-10
- 172.17.1.102 — KAN-11
- 172.17.1.2 — KAN-12

DONE 3 ✓

- Nessus Inventory — ~~KAN-1~~
- WAZUH Inventory — ~~KAN-2~~
- Splunk Vulnerability Management — ~~KAN-3~~



172.16.1.5

Description

High - 7.5 - 5.1 - 0.0398 - 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Activity

Michael Kohronas 10 seconds ago

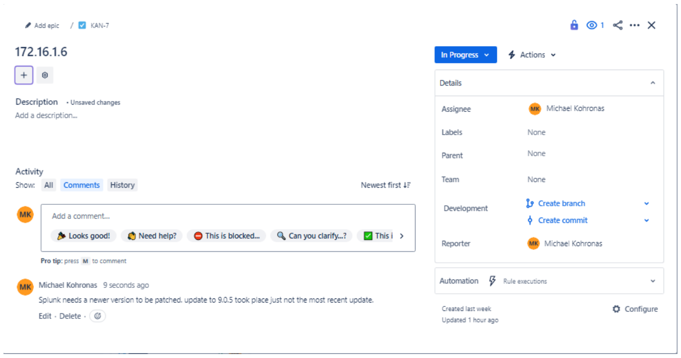
SWEET32 persist after added SCHANNEL, ciphers, Triple DES 168

Details

Assignee	MK Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	MK Michael Kohronas

Automation — Rule executions

Created last week
Updated 1 hour ago



172.16.1.6

Description • Unsaved changes

Add a description...

Activity

Michael Kohronas 9 seconds ago

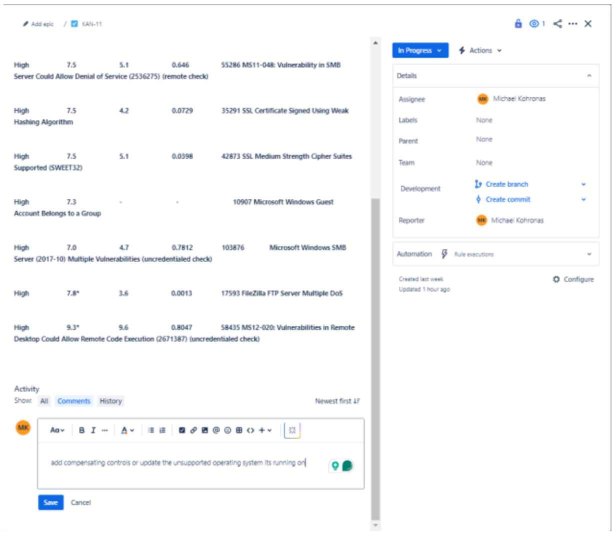
Splunk needs a newer version to be patched. update to 9.0.5 took place just not the most recent update.

Details

Assignee	MK Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	MK Michael Kohronas

Automation — Rule executions

Created last week
Updated 1 hour ago



Add epic / KAN-11

High	7.5	5.1	0.646	55286 MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275) (remote check)
High	7.5	4.2	0.0729	35291 SSL Certificate Signed Using Weak Hashing Algorithm
High	7.5	5.1	0.0398	42873 SSL Medium Strength Cipher Suites Supported (SWEET32)
High	7.3	-	-	10907 Microsoft Windows Guest Account Belongs to a Group
High	7.0	4.7	0.7812	103876 Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High	7.8*	3.6	0.0013	17593 FileZilla FTP Server Multiple DoS
High	9.3*	9.6	0.8047	58435 MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Activity
Show: All Comments History Newest first

MK add compensating controls or update the unsupported operating system its running on

Save Cancel

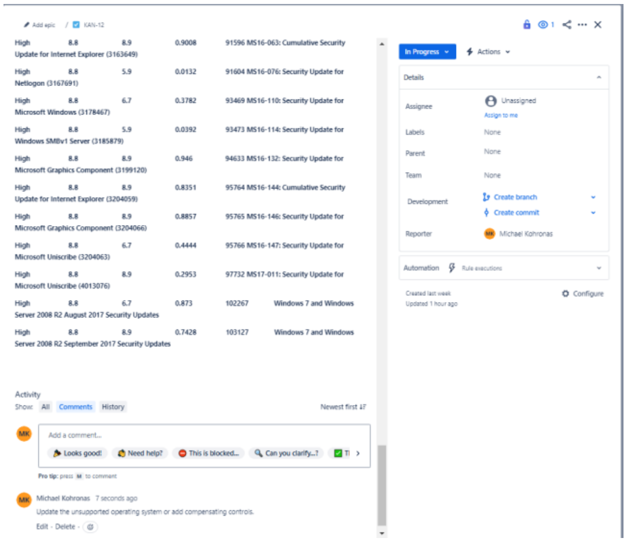
In Progress Actions

Details

Assignee	MK Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	MK Michael Kohronas

Automation Rule executions

Created last week
Updated 1 hour ago
Configure



Add epic / KAN-12

High	8.8	8.9	0.9008	91596 MS16-063: Cumulative Security Update for Internet Explorer (3163649)
High	8.8	5.9	0.0132	91604 MS16-076: Security Update for Netlogon (3167691)
High	8.8	6.7	0.3782	93469 MS16-110: Security Update for Microsoft Windows (3178467)
High	8.8	5.9	0.0392	93473 MS16-114: Security Update for Windows SMBv1 Server (3185879)
High	8.8	8.9	0.946	94633 MS16-132: Security Update for Microsoft Graphics Component (3199120)
High	8.8	8.9	0.8351	95764 MS16-144: Cumulative Security Update for Internet Explorer (3204059)
High	8.8	8.9	0.8857	95765 MS16-146: Security Update for Microsoft Graphics Component (3204066)
High	8.8	6.7	0.4444	95766 MS16-147: Security Update for Microsoft Uniscribe (3204063)
High	8.8	8.9	0.2953	97732 MS17-011: Security Update for Microsoft Uniscribe (4013076)
High	8.8	6.7	0.873	102267 Windows 7 and Windows Server 2008 R2 August 2017 Security Updates
High	8.8	8.9	0.7428	103127 Windows 7 and Windows Server 2008 R2 September 2017 Security Updates

Activity
Show: All Comments History Newest first

MK Add a comment...
Looks good! Need help? This is blocked... Can you clarify...? Ti

Pro tip: press M to comment

MK Michael Kohronas 7 seconds ago
Update the unsupported operating system or add compensating controls.
Edit · Delete ·

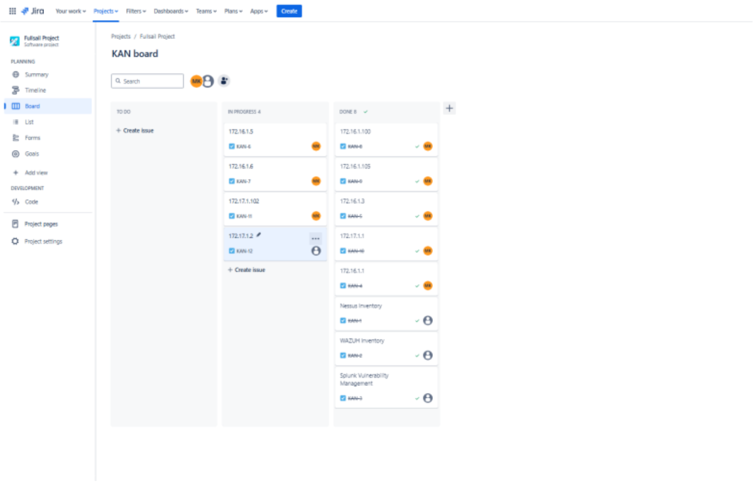
In Progress Actions

Details

Assignee	Unassigned Assign to me
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	MK Michael Kohronas

Automation Rule executions

Created last week
Updated 1 hour ago
Configure



Projects / Fullsail Project

KAN board

TO DO	IN PROGRESS 4	DONE 8 ✓
+ Create issue	172.16.1.5 KAN-6 MK	172.16.1.100 ~~KAN-8~~ ✓ MK
	172.16.1.6 KAN-7 MK	172.16.1.105 ~~KAN-9~~ ✓ MK
	172.17.1.102 KAN-11 MK	172.16.1.3 ~~KAN-5~~ ✓ MK
	172.17.1.2 KAN-12	172.17.1.1 ~~KAN-10~~ ✓ MK
	+ Create issue	172.16.1.1 ~~KAN-4~~ ✓ MK
		Nessus Inventory ~~KAN-1~~ ✓
		WAZUH Inventory ~~KAN-2~~ ✓
		Splunk Vulnerability Management ~~KAN-3~~ ✓