Qualys. Cloud Platform

10.132.33.175

March 17, 2022

Report Summary	
User Name:	Rajesh Tripathi
Login Name:	nc_rt
Company:	NIC
User Role:	Manager
Address:	A-Block,Lodhi Rd,CGO Complex
City:	New Delhi
State:	Delhi
Zip:	110003
Country:	India
Created:	03/17/2022 at 03:42:00 PM (GMT+0530)
Template Title:	NIC exclude
Asset Groups:	-
IPs:	10.132.33.175
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01/01/1999 - 03/17/2022
Active Hosts:	2
Hosts Matching Filters:	2

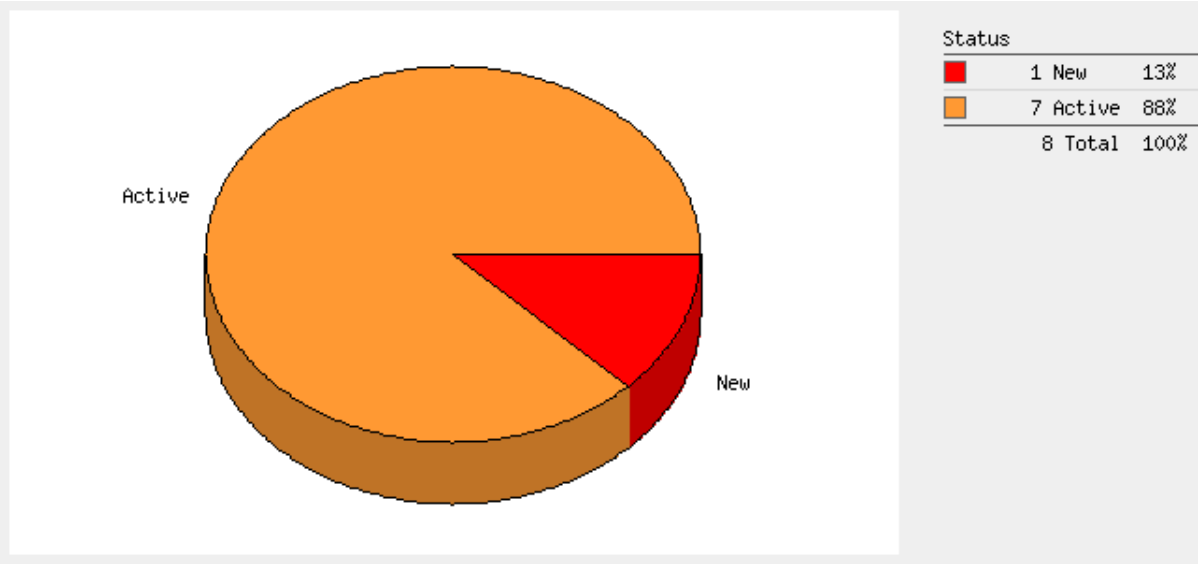
Summary of Vulnerabilities

Vulnerabilities Total	8	Security Risk (Avg)	2.5	Business Risk	64/100

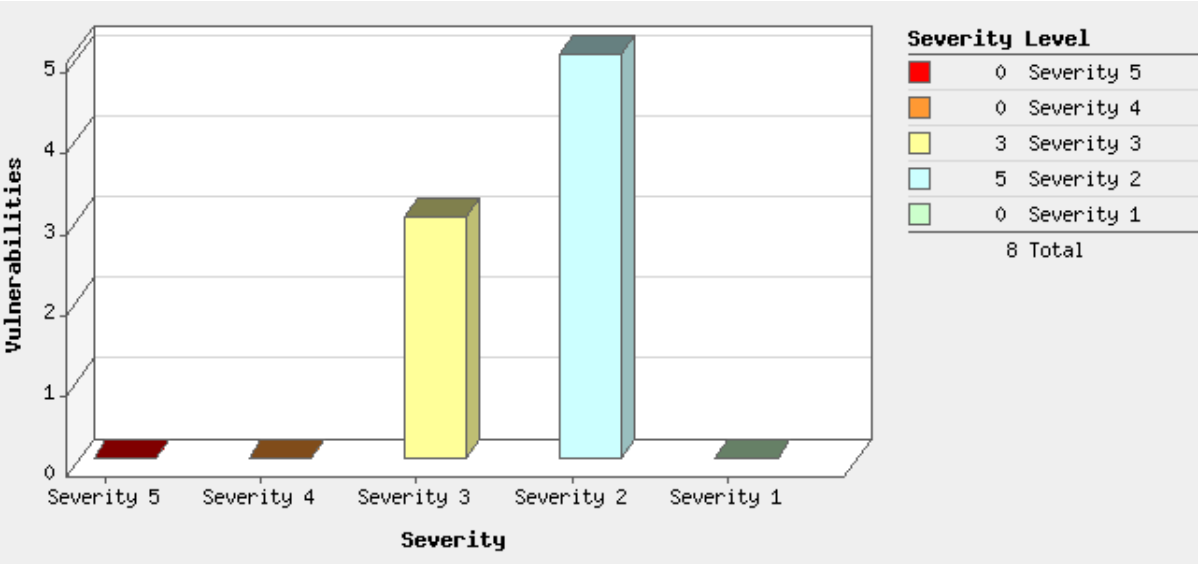
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	3	-	-	3
2	5	-	-	5
1	0	-	-	0
Total	8	-	-	8

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Windows	4	-	-	4
Security Policy	3	-	-	3
CGI	1	-	-	1
Total	8	-	-	8

Vulnerabilities by Status



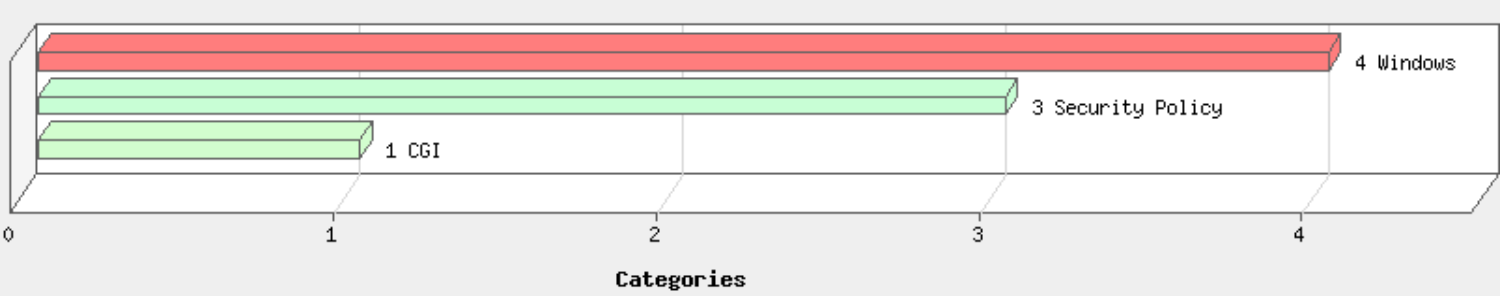
Vulnerabilities by Severity



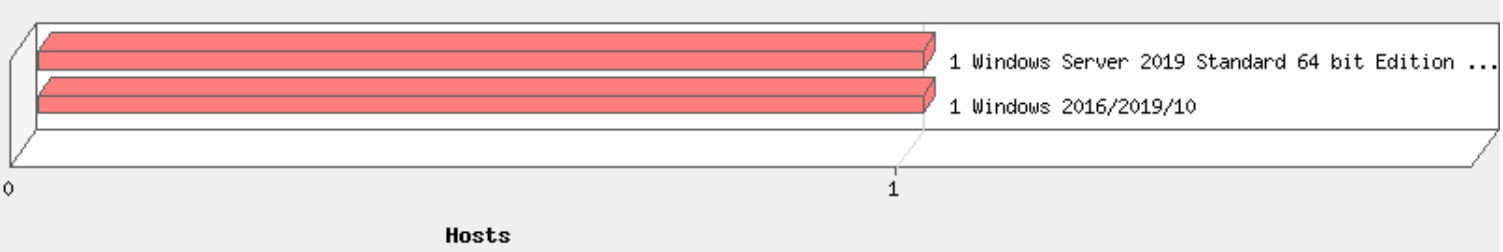
Information Gathered by Severity

There are no known vulnerabilities for this/these systems

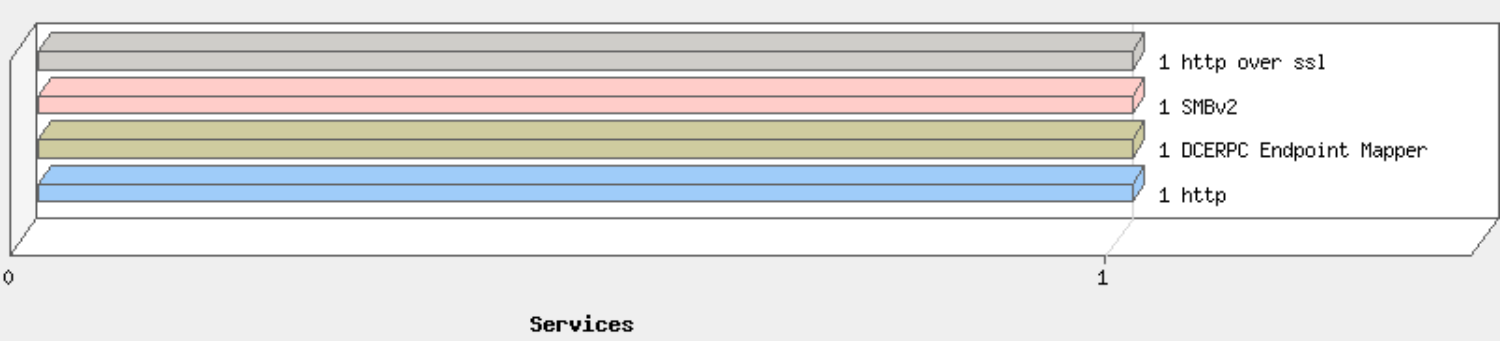
Top 5 Vulnerable Categories



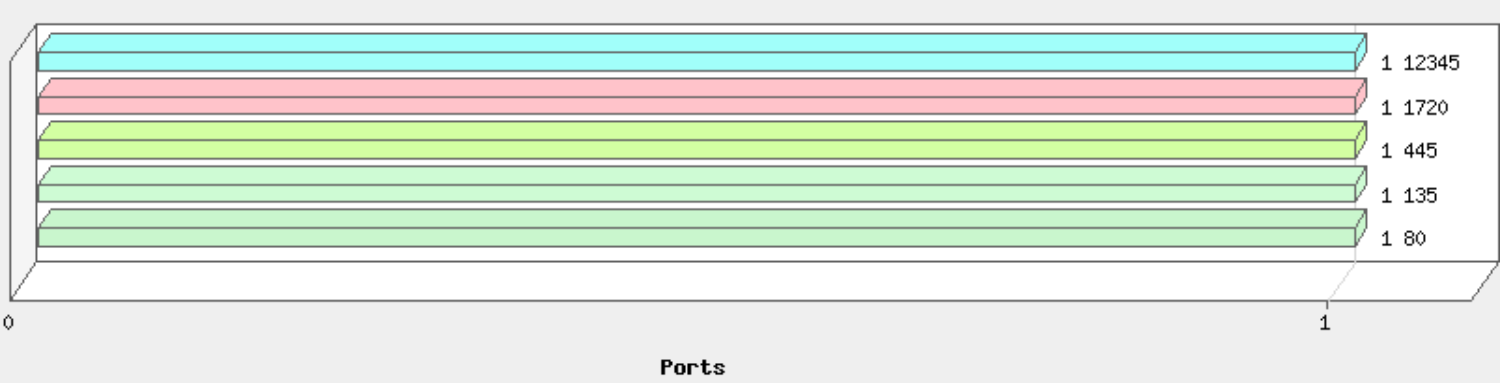
Operating Systems Detected



Services Detected



Ports Detected



Detailed Results

10.132.33.175 (win-ocmrck93fp2, WIN-OCMRCK93FP2) Windows 2016/2019/10

Host Identification Information
IPs
QG Host ID

Vulnerabilities Total	1	Security Risk	2.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	0	-	-	0
2	1	-	-	1
1	0	-	-	0
Total	1	-	-	1

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
CGI	1	-	-	1
Total	1	-	-	1

Vulnerabilities (1)

2 HTTP Security Header Not Detected port 80/tcp New

QID: 11827
Category: CGI
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/27/2022
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

First Detected: 03/15/2022 at 03:57:19 PM (GMT+0530)
Last Detected: 03/15/2022 at 03:57:19 PM (GMT+0530)
Times Detected: 1
Last Fixed: N/A

THREAT:

This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers) according to CWE-693: Protection Mechanism Failure (https://cwe.mitre.org/data/definitions/693.html):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
The Valid directives are as belows:
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -IkL --verbose.
CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Customers are advised to set proper X-Content-Type-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) and Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) HTTP response headers.
Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:
X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff
HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;
Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

RESULTS:

X-Content-Type-Options HTTP Header missing on port 80.

GET / HTTP/1.0
Host: 10.132.33.175

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 22 Sep 2021 06:52:18 GMT
Accept-Ranges: bytes
ETag: "5e3ab7627eafd71:0"
Server: Microsoft-IIS/10.0
Date: Tue, 15 Mar 2022 10:01:08 GMT
Connection: keep-alive
Content-Length: 703

10.132.33.175 (win-ocmrck93fp2, WIN-OCMRCK93FP2) Windows Server 2019 Standard 64 bit Editio...

Host Identification Information	
IPs	
QG Host ID	57939e00-dc9e-409b-924e-84cdb9a5a94c

Vulnerabilities Total	7	Security Risk	3.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	3	-	-	3
2	4	-	-	4
1	0	-	-	0
Total	7	-	-	7

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Windows	4	-	-	4
Security Policy	3	-	-	3
Total	7	-	-	7

Vulnerabilities (7)

3 Built-in Guest Account Not Renamed at Windows Target System — Active

QID: 105228
Category: Security Policy
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/12/2019
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 03/16/2022 at 03:03:44 PM (GMT+0530)
Last Detected: 03/17/2022 at 02:05:06 PM (GMT+0530)
Times Detected: 6
Last Fixed: N/A

THREAT:
The built-in Guest account is not renamed at the target Microsoft Windows system.

IMPACT:
Knowing a valid username allows for substantially easier bruteforcing attacks.

SOLUTION:
Rename the Guest account.

RESULTS:
Guest

3 Allowed Null Session — Active

QID: 90044
Category: Windows
Associated CVEs: CVE-2002-1117, CVE-2000-1200
Vendor Reference: -
Bugtraq ID: 494, 959
Service Modified: 03/03/2022
User Modified: -
Edited: No
PCI Vuln: Yes

Ticket State:

First Detected: 03/16/2022 at 03:03:44 PM (GMT+0530)

Last Detected: 03/17/2022 at 02:05:06 PM (GMT+0530)

Times Detected: 6

Last Fixed: N/A

THREAT:

It is possible to log into the target host using a NULL session.
Windows NT has a feature allowing anonymous users to obtain domain user names and the share list. Windows NT ACL editor requires the Domain Controllers to return a list of account names.
We check for "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA RestrictAnonymous" as well as "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters RestrictNullSessAccess" = 0 as Microsoft has stated that "Remote access to the registry may still be possible after you follow the steps in this article if the RestrictNullSessAccess registry value has been created and is set to 0. This value allows remote access to the registry by using a null session. The value overrides other explicit restrictive settings."

IMPACT:

Unauthorized users can establish a null session and obtain sensitive information, such as usernames and/or the share list, which could be used in further attacks against the host.

SOLUTION:

To disable or restrict null session, please refer to Microsoft Knowledge Base Article For restricting-information-available-to-anonymous-logon-users (https://support.microsoft.com/en-us/help/143474/restricting-information-available-to-anonymous-logon-users) or Microsoft TechNet : RestrictNullSessAccess (https://technet.microsoft.com/en-us/library/cc957461.aspx) for further details.

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\LSA RestrictAnonymous = 0

3 SMB Signing Disabled or SMB Signing Not Required Active

QID:	90043
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/09/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

Ticket State:

First Detected: 03/16/2022 at 03:03:44 PM (GMT+0530)

Last Detected: 03/17/2022 at 02:05:06 PM (GMT+0530)

Times Detected: 6

Last Fixed: N/A

THREAT:

This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.
SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.
When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.
QID Detection Logic:
This checks from the registry value of RequireSecuritySignature and EnableSecuritySignature form HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkStation\Parameters for client and HKEY_LOCAL_MACHINE\System\CurrentControlSetServices\LanmanServer\Parameters for servers to check if SMB signing is required or enabled or disabled.
Note: On 5/28/2020 the QID was updated to check for client SMB signing behavior via the registry key HKEY_LOCAL_MACHINE\SystemCurrent\ControlSetServices\LanmanWorkStation\Parameters. The complete detection logic is explained above.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys,

and then authenticate on the Domain Controller.

SOLUTION:
Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.
Please refer to Microsoft's article 887429 (http://support.microsoft.com/kb/887429) and The Basics of SMB Signing (covering both SMB1 and SMB2) (https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2) for information on enabling SMB signing.
For Windows Server 2008 R2, Windows Server 2012, please refer to Microsoft's article Require SMB Security Signatures (http://technet.microsoft.com/en-us/library/cc731957.aspx) for information on enabling SMB signing. For group policies please refer to Microsoft's article Modify Security Policies in Default Domain Controllers Policy (http://technet.microsoft.com/en-us/library/cc731654)
For UNIX systems
To require samba clients running "smbclient" to use packet signing, add the following to the "[global]" section of the Samba configuration file:
client signing = mandatory

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters requiresecuritysignature = 0
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters enablesecuritysignature = 0

2 Enabled Cached Logon Credential — Active

QID:	90007
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/06/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	

First Detected: 03/16/2022 at 03:03:44 PM (GMT+0530)

Last Detected: 03/17/2022 at 02:05:06 PM (GMT+0530)

Times Detected: 6

Last Fixed: N/A

THREAT:
Windows NT may use a cache to store the last interactive logon (i.e. console logon), to provide a safe logon for the host in the event that the Domain Controller goes down. This feature is currently activated on this host.

IMPACT:
Unauthorized users can gain access to this cached information, thereby obtaining sensitive logon information.

SOLUTION:
We recommend that you locate the following Registry key, and then set or create a REG_SZ 'CachedLogonsCount' entry with a '0' value:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Nt\CurrentVersion\Winlogon

RESULTS:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon cachedlogonscount = 10

2 Microsoft Windows Explorer AutoPlay Not Disabled — Active

QID:	105170
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/14/2009
User Modified:	-
Edited:	No

PCI Vuln: Yes
Ticket State:

First Detected: 03/16/2022 at 03:03:44 PM (GMT+0530)
Last Detected: 03/17/2022 at 02:05:06 PM (GMT+0530)
Times Detected: 6
Last Fixed: N/A

THREAT:
The setting that prevents applications from any drive to be automatically executed is not enabled on the host.

IMPACT:
Exploiting this vulnerability can cause malicious applications to be executed unintentionally at escalated privilege.

SOLUTION:
Disable autoplay from any disk type by setting the value NoDriveTypeAutoRun to 255 under this registry key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

RESULTS:
%windir%\explorer.exe found
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveTypeAutoRun is missing.

2 Windows Explorer Autoplay Not Disabled for Default User Active

QID: 105171
Category: Security Policy
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/10/2019
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

First Detected: 03/16/2022 at 03:03:44 PM (GMT+0530)
Last Detected: 03/17/2022 at 02:05:06 PM (GMT+0530)
Times Detected: 6
Last Fixed: N/A

THREAT:
The setting that prevents applications from any drive to be automatically executed when no user is logged in is not enabled on the host.

IMPACT:
An attacker may be able to run an unauthorized application.

SOLUTION:
Make sure that the value NoDriveTypeAutoRun is defined under this registry key:
HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

RESULTS:
%windir%\explorer.exe found
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoAutorun is missing.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveTypeAutoRun is missing.
HKU\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer NoDriveTypeAutoRun is missing.

2 Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4) Active

QID: 91462

Category:	Windows
Associated CVEs:	CVE-2018-3639
Vendor Reference:	ADV180012
Bugtraq ID:	104232
Service Modified:	02/04/2022
User Modified:	02/04/2022
Edited:	Yes
PCI Vuln:	No
Ticket State:	

First Detected: 03/16/2022 at 03:03:44 PM (GMT+0530)

Last Detected: 03/17/2022 at 02:05:06 PM (GMT+0530)

Times Detected: 6

Last Fixed: N/A

THREAT:

On January 3 2018, Microsoft released an advisory and security updates related to hardware vulnerabilities (known as Spectre and Meltdown) involving speculative execution side channels that affect AMD, ARM, and Intel CPUs to varying degrees.
On May 21st, a new subclass of speculative execution side channel vulnerabilities known as Speculative Store Bypass (SSB) has been announced and assigned CVE-2018-3639.
The Windows registry key settings are missing on the target.
Microsoft requires you to apply the following Registry Key settings in addition to Windows Patch

To enable the fix:

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 8 /f
OR
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 72 /f
OR
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 8264 /f
AND
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f

For more information regarding this QID please refer to our community blog post - Details for Mitigating Speculative Store Bypass (SSB) - CVE-2018-3639 (https://community.qualys.com/docs/DOC-6531-details-for-mitigating-speculative-store-bypass-ssb-cve-2018-3639)
QID Detection Logic (Authenticated):
Operating Systems: Windows Server 2008 R2, Windows 7, Windows 8.1, Windows10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016,Windows Server 2019
This QID checks for the presence of following Registry key Value and if these registries are missing or values are wrong then this QID is flagged:
Reg Key - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management, Value - FeatureSettingsOverride, REG DWORD - "8264" or "72" or "8"
Reg Key - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management, Value - FeatureSettingsOverrideMask, REG DWORD - "3"

IMPACT:

An attacker who has successfully exploited this vulnerability may be able to read privileged data across trust boundaries. Vulnerable code patterns in the operating system (OS) or in applications could allow an attacker to exploit this vulnerability. In the case of Just-in-Time (JIT) compilers, such as JavaScript JIT employed by modern web browsers, it may be possible for an attacker to supply JavaScript that produces native code that could give rise to an instance of CVE-2018-3639.

SOLUTION:

Customers are advised to refer to ADV180012 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180012) for more details pertaining to this vulnerability.
Please refer to the section "Enabling protections on the server" from the Microsoft link for Server Operating systems (https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution), Microsoft link for Client Operating Systems (https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in) for more details

Patch:
Following are links for downloading patches to fix the vulnerabilities:
ADV180012 (https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in)
ADV180012 (https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution)

RESULTS:

HKLM\System\CurrentControlSet\Control\Session Manager\Environment PROCESSOR_IDENTIFIER = Intel64 Family 6 Model 63 Stepping 0, GenuineIntel
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management FeatureSettingsOverride is missing.
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management FeatureSettingsOverrideMask is missing.
