Finding Vulnerability using Nessus Assignment

Erika Hernandez

IT-6370 Summer 2023

Windows 2008

High

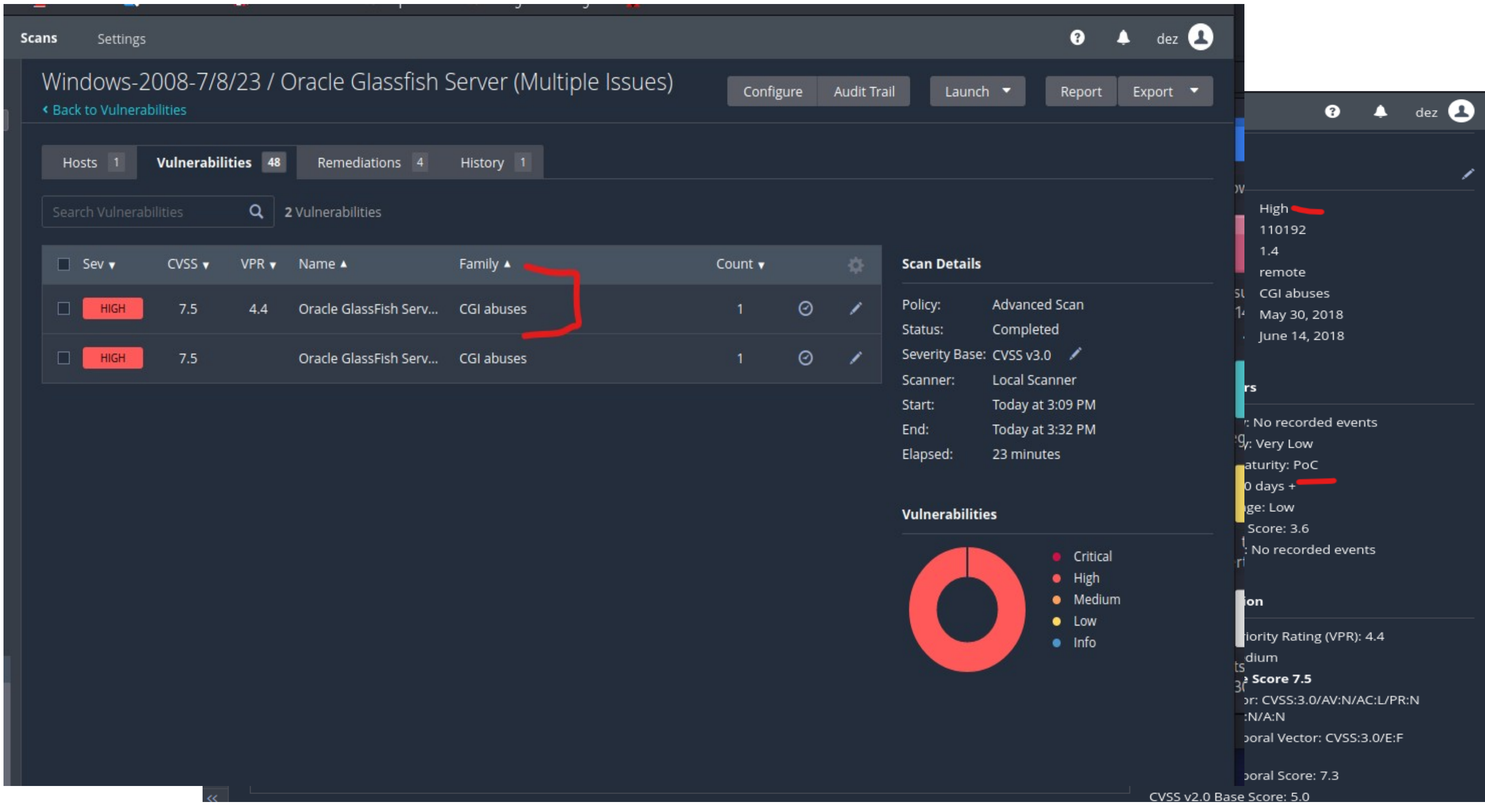
Oracle GlassFish Server Path Traversal

Description

The instance of Oracle GlassFish Server running on the remote host is affected by an authenticated and unauthenticated path traversal vulnerability. Remote attacker can exploit this issue, via a specially crafted HTTP request, to access arbitrary files on the remote host.

CVE-2017-1000028

https://nvd.nist.gov/vuln/detail/CVE-2017-1000028



Windows-2008-7/8/23 / Oracle Glassfish Server (Multiple Issues)

2 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
HIGH	7.5	4.4	Oracle GlassFish Serv...	CGI abuses	1
HIGH	7.5		Oracle GlassFish Serv...	CGI abuses	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:09 PM
End: Today at 3:32 PM
Elapsed: 23 minutes

Vulnerabilities

High
110192
1.4
remote
CGI abuses
May 30, 2018
June 14, 2018

rs

: No recorded events
y: Very Low
aturity: PoC
0 days +
ge: Low
Score: 3.6
: No recorded events

ion

iority Rating (VPR): 4.4
dium
Score 7.5
or: CVSS:3.0/AV:N/AC:L/PR:N
:N/A:N
oral Vector: CVSS:3.0/E:F
oral Score: 7.3
CVSS v2.0 Base Score: 5.0

Summary:

The CVE-2017-1000028 vulnerability refers to a security flaw found in Oracle's GlassFish Server Open Source Edition version 4.1. This vulnerability allows an attacker to perform a type of attack called Directory Traversal.

Directory Traversal is a technique used by attackers to access files and directories on a web server that should not be publicly accessible. By exploiting this vulnerability, an attacker can manipulate a specially crafted HTTP GET request to bypass security restrictions and access files or directories outside the intended scope. This could potentially lead to unauthorized disclosure of sensitive information, unauthorized modifications, or even a complete compromise of the system.

It is important to fix this vulnerability because it poses a security risk to the affected system. By exploiting this flaw, an attacker can gain unauthorized access to sensitive files, compromise the server's integrity, and potentially launch further attacks. Fixing the vulnerability involves patching or updating the affected software to a version that addresses the security issue. This helps to ensure the system's security and protect it from potential attacks.

Fixes: Check for available patches or updates. Visit the official Oracle website or the GlassFish Server documentation to check for any available patches, updates, or security advisories specifically addressing the CVE-2017-1000028 vulnerability. Look for any recommended actions or instructions provided by Oracle.

Windows XP

Critical

Microsoft Windows XP Unsupported Installation Detection

Description

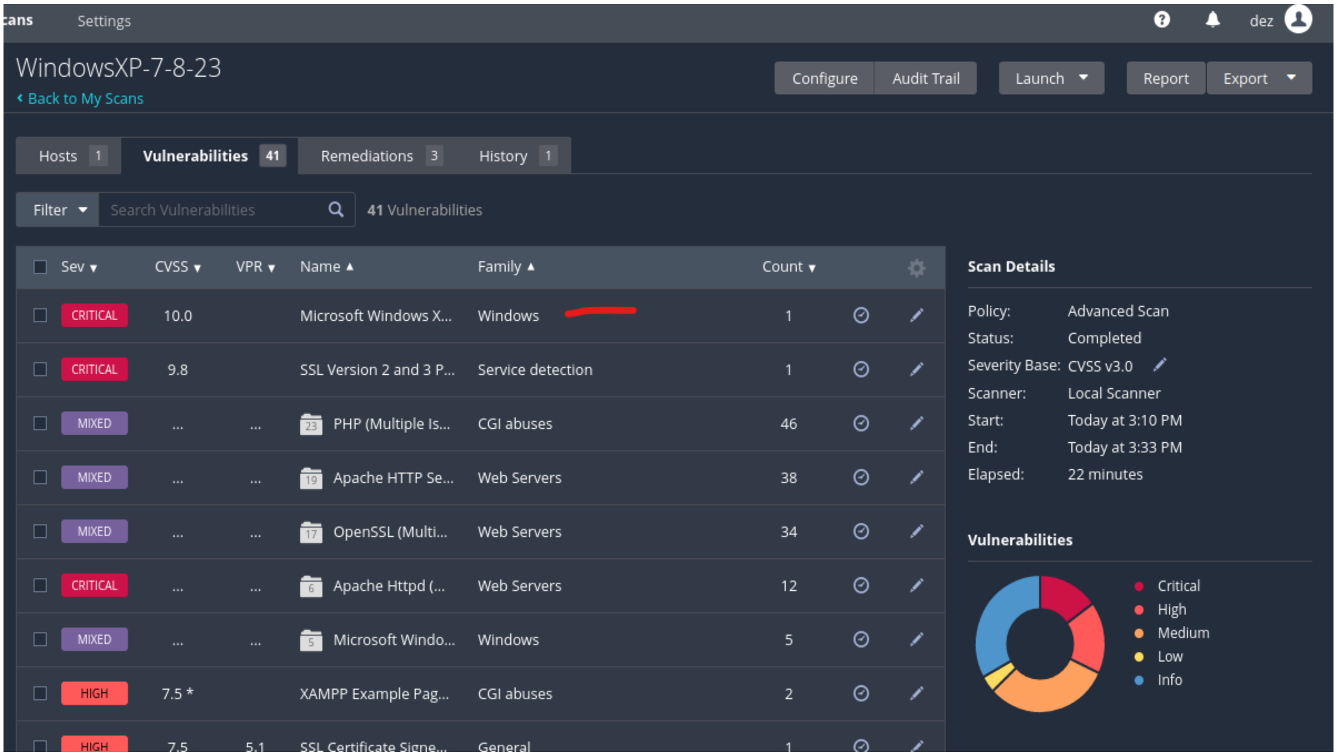
The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

CVE: Not specified but important.

https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

https://www.cisa.gov/news-events/alerts/2017/01/16/smb-security-best-practices



WindowsXP-7-8-23

‹ Back to My Scans

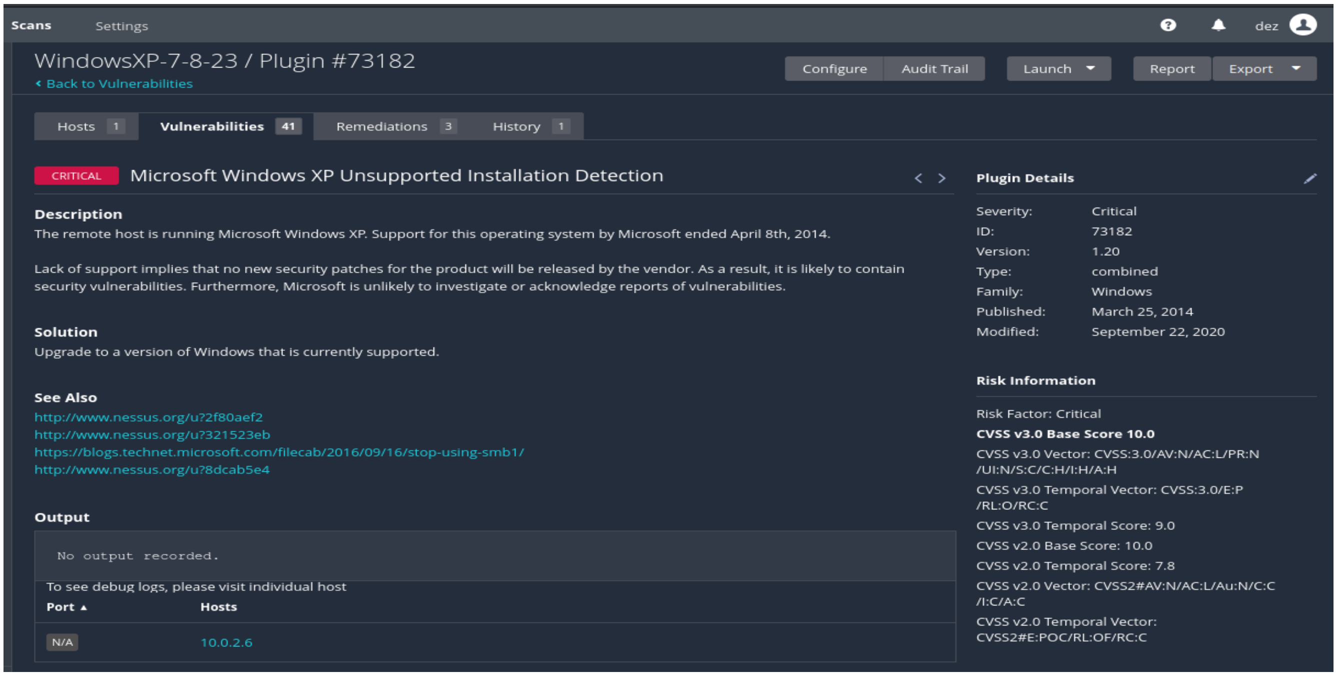
41 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾
CRITICAL	10.0		Microsoft Windows X...	Windows	1
CRITICAL	9.8		SSL Version 2 and 3 P...	Service detection	1
MIXED	...	...	23 PHP (Multiple Is...	CGI abuses	46
MIXED	...	...	19 Apache HTTP Se...	Web Servers	38
MIXED	...	...	17 OpenSSL (Multi...	Web Servers	34
CRITICAL	...	...	6 Apache Httpd (...	Web Servers	12
MIXED	...	...	5 Microsoft Windo...	Windows	5
HIGH	7.5 *		XAMPP Example Pag...	CGI abuses	2
HIGH	7.5	5.1	SSL Certificate Signe...	General	1

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 3:10 PM
End:	Today at 3:33 PM
Elapsed:	22 minutes

Vulnerabilities



WindowsXP-7-8-23 / Plugin #73182

‹ Back to Vulnerabilities

CRITICAL Microsoft Windows XP Unsupported Installation Detection

Description

The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

Solution

Upgrade to a version of Windows that is currently supported.

See Also

http://www.nessus.org/u?2f80aef2
http://www.nessus.org/u?321523eb
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
http://www.nessus.org/u?8dcab5e4

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▴	Hosts
N/A	10.0.2.6

Plugin Details

Severity:	Critical
ID:	73182
Version:	1.20
Type:	combined
Family:	Windows
Published:	March 25, 2014
Modified:	September 22, 2020

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.0
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 7.8
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

Summary:

The description states that the remote host (a computer system) is running Microsoft Windows XP, which is an outdated operating system. It further mentions that support for Windows XP ended on April 8th, 2014.

When an operating system is no longer supported, it means that the manufacturer (in this case, Microsoft) no longer releases security patches or updates to address vulnerabilities or bugs. As a result, the operating system is more likely to have security vulnerabilities that can be exploited by attackers.

Fixes: The solution to this issue is to upgrade to a currently supported version of the Windows operating system. By upgrading to a newer version, you will have access to the latest security patches, updates, and support from Microsoft. This helps to ensure that your system remains protected against known vulnerabilities and keeps your data and information secure.

Metasploitable Linux 2

Critical

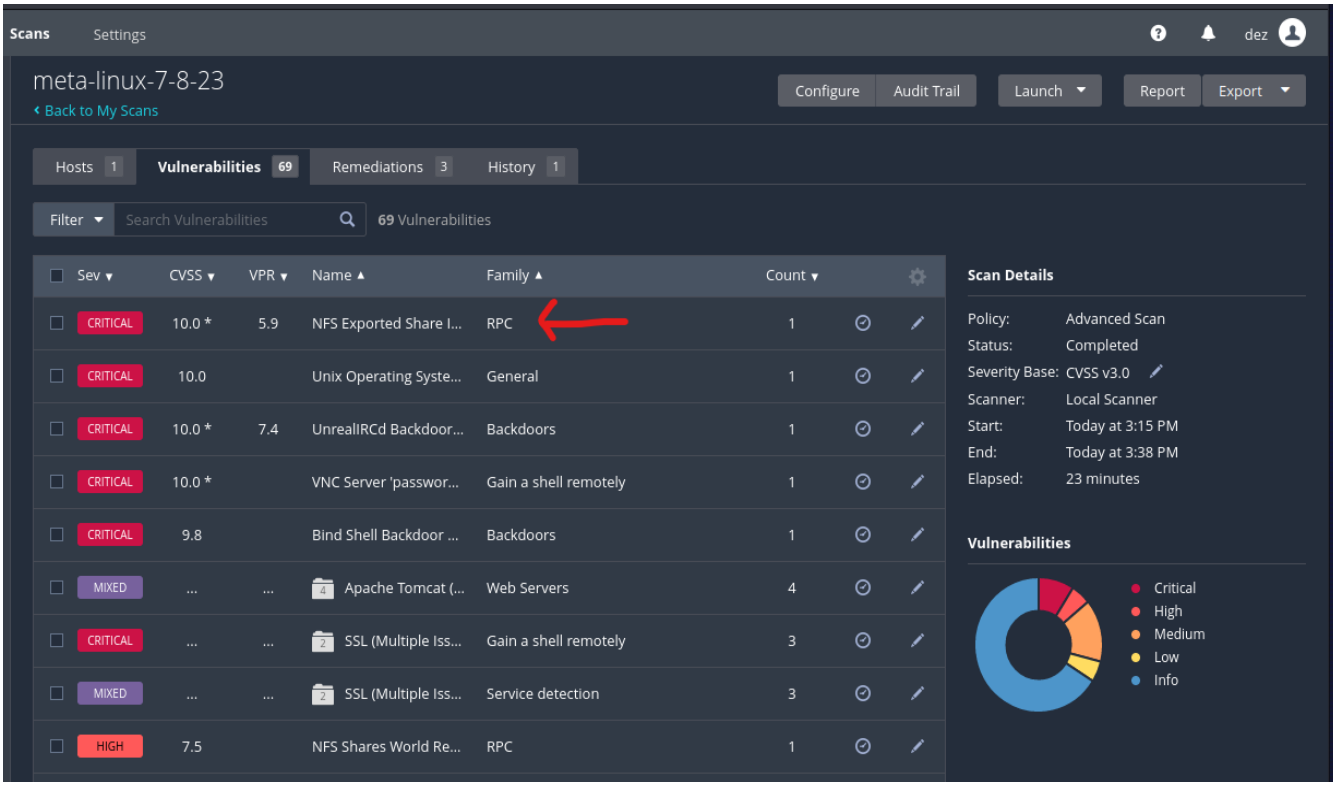
NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

CVE: CVE-1999-0554, CVE-1999-0211, CVE-1999-0170

https://nvd.nist.gov/vuln/detail/CVE-1999-0554
https://nvd.nist.gov/vuln/detail/CVE-1999-0211
https://nvd.nist.gov/vuln/detail/CVE-1999-0170



meta-linux-7-8-23

‹ Back to My Scans

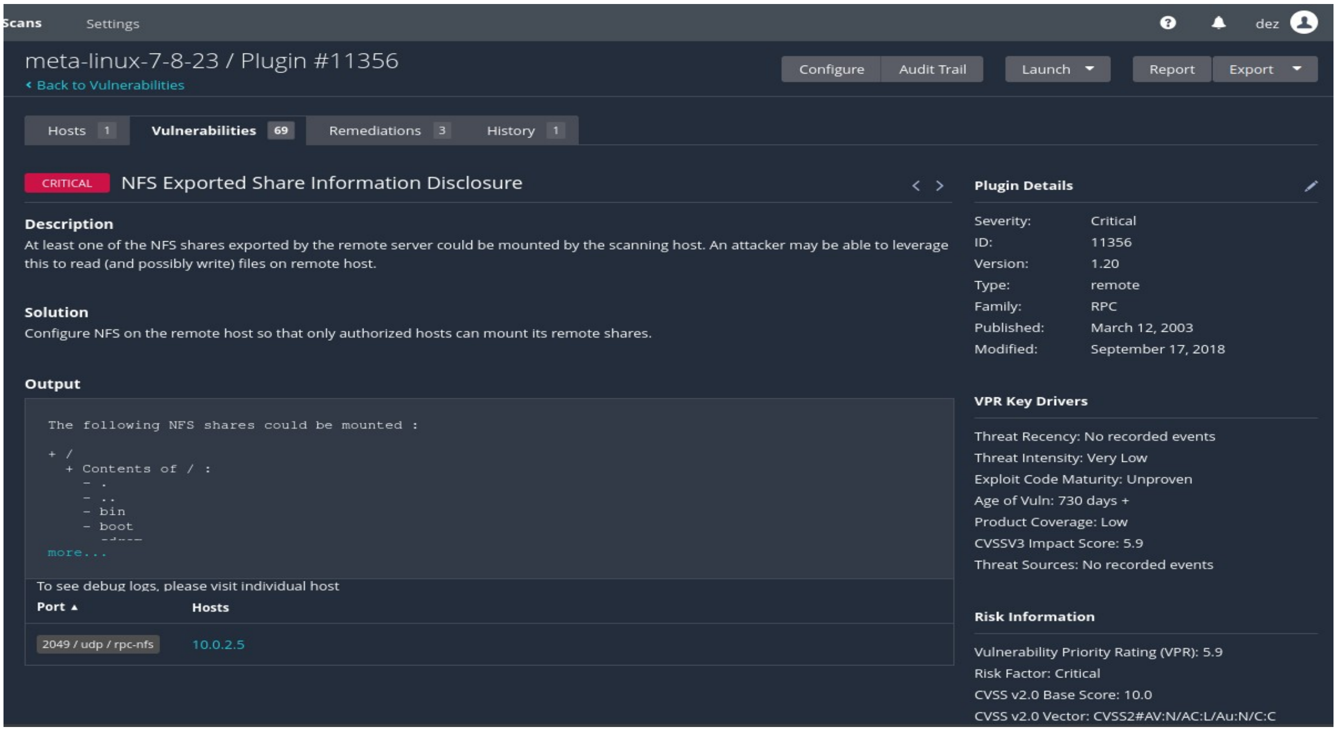
69 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share I...	RPC	1
CRITICAL	10.0		Unix Operating Syste...	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor...	Backdoors	1
CRITICAL	10.0 *		VNC Server 'passwor...	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Backdoor ...	Backdoors	1
MIXED	...	...	4 Apache Tomcat (...	Web Servers	4
CRITICAL	...	...	2 SSL (Multiple Iss...	Gain a shell remotely	3
MIXED	...	...	2 SSL (Multiple Iss...	Service detection	3
HIGH	7.5		NFS Shares World Re...	RPC	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:15 PM
End: Today at 3:38 PM
Elapsed: 23 minutes

Vulnerabilities



meta-linux-7-8-23 / Plugin #11356

‹ Back to Vulnerabilities

NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	10.0.2.5

Plugin Details

Severity:	Critical
ID:	11356
Version:	1.20
Type:	remote
Family:	RPC
Published:	March 12, 2003
Modified:	September 17, 2018

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C

Summary:

This vulnerability described is related to NFS (Network File System) on a remote server. NFS allows files to be shared and accessed over a network. The vulnerability suggests that at least one of the NFS shares on the remote server is configured in a way that allows it to be mounted by the scanning host (the system performing the vulnerability scan). This means that an attacker who can access the scanning host may be able to read and possibly modify files on the remote server.

Fixes: To fix this vulnerability, you need to configure NFS on the remote server to restrict access to authorized hosts only. By putting proper access controls, you can ensure that only trusted systems are allowed to mount the NFS shares and access the files.

- Review and update the NFS configuration: Open the NFS configuration file using a text editor and review the existing entries. Make sure that only the necessary shares are exported and that the access permissions are properly set.

- Restrict access to authorized hosts: Modify the NFS configuration to specify the IP addresses or hostnames of the authorized systems that are allowed to mount the NFS shares. Remove any overly permissive settings that could allow unauthorized access.

In Closing

Overall, I would like to say that this was a very good assignment. The videos were very helpful in completing this assignment. I would like to reiterate that this could be a full-time job, both for ensuring the infrastructure security and for the person carrying out the attacks. Having all these tools makes things easier, but if you don't know which tools to use, you won't be able to protect the company.

Therefore, it would be easier for a small company to hire or outsource this cybersecruity work to companies. In order to search for all these vulnerabilities, you really need to stay on top of everything. You have to constantly search for systems and perform scans. Then, you have to go to the server and patch any vulnerabilities you find. This is very important, which is why outsourcing or having a dedicated team solely focused on this is beneficial. It can be quite intimidating, so looking into this is very important to ensure security because it only takes a small window of opportunity for an attack to occur.

I must say that after taking this class with you in the spring and now again, my eyes have been opened to so much. I want to make sure that the company I currently work for or any future company I work for can utilize these tools that you have been showing us. I think this is great, and it's amazing to see these scans in action.