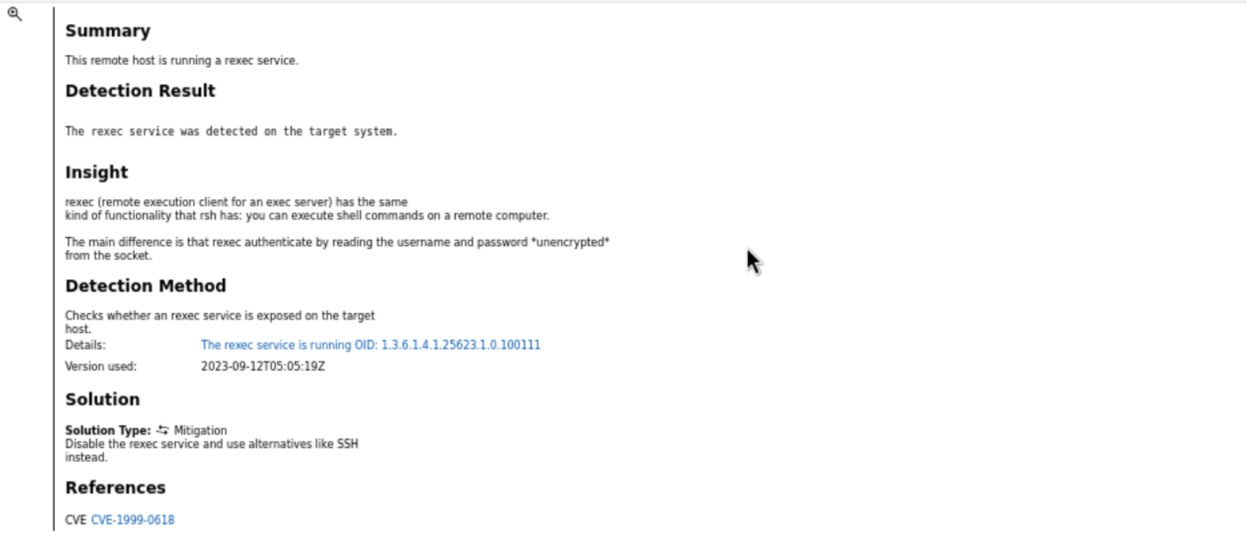
Questions

For each vulnerability you fixed give the following information:

1. CVE-1999-0618



Summary

This remote host is running a rexec service.

Detection Result

```
The rexec service was detected on the target system.
```

Insight

rexec (remote execution client for an exec server) has the same
kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticate by reading the username and password *unencrypted*
from the socket.

Detection Method

Checks whether an rexec service is exposed on the target
host.

Details: The rexec service is running OID: 1.3.6.1.4.1.25623.1.0.100111

Version used: 2023-09-12T05:05:19Z

Solution

Solution Type: Mitigation
Disable the rexec service and use alternatives like SSH
instead.

References

CVE CVE-1999-0618

Severity Rating: 10

What danger the CVE presents to the system

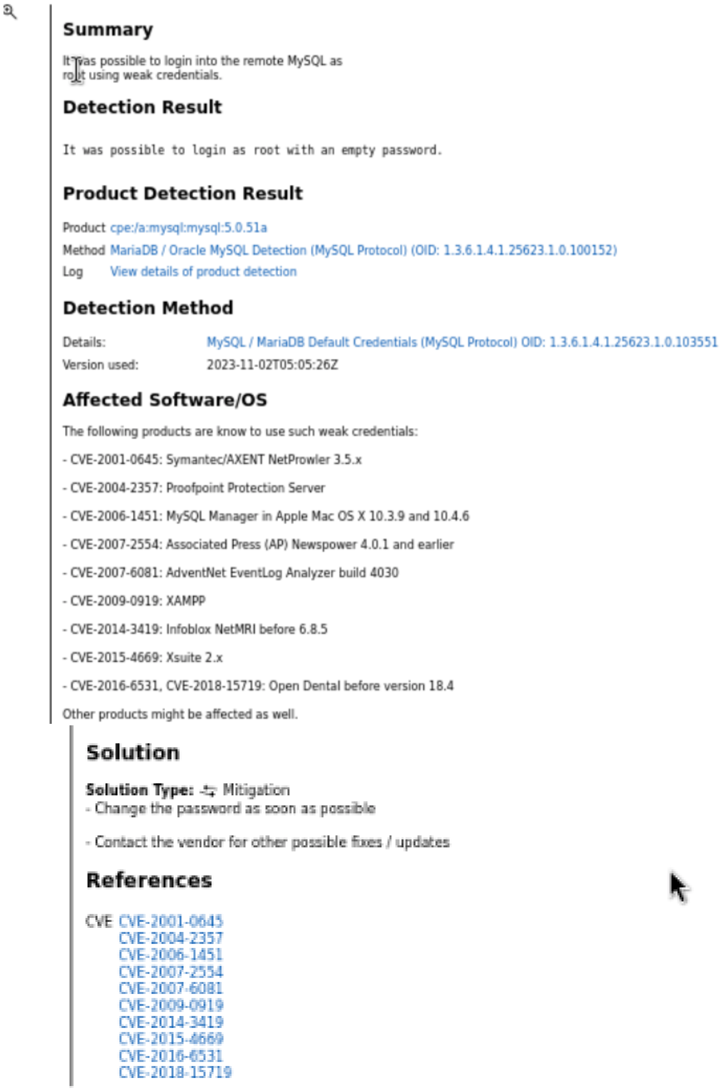
This service allows remote command execution on a host but uses unencrypted methods for authentication. When users connect to the service, their username and password are transmitted in plaintext across the network. This makes it easy for attackers to intercept these credentials using packet sniffing tools, exposing the system to unauthorized access.

What you did to fix it

I fixed it by sudo nano /etc/inetd.conf and disabled it by adding a # at the beginning of the execs service. Then I enabled SSH service. And then, I rebooted the server.

2. SQL

CVE CVE-2001-0645
CVE-2004-2357
CVE-2006-1451
CVE-2007-2554
CVE-2007-6081
CVE-2009-0919
CVE-2014-3419
CVE-2015-4669
CVE-2016-6531
CVE-2018-15719



Summary

It was possible to login into the remote MySQL as
root using weak credentials.

Detection Result

```
It was possible to login as root with an empty password.
```

Product Detection Result

Product cpe:/a:mysql:mysql:5.0.51a
Method MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.25623.1.0.100152)
Log View details of product detection

Detection Method

Details: MySQL / MariaDB Default Credentials (MySQL Protocol) OID: 1.3.6.1.4.1.25623.1.0.103551
Version used: 2023-11-02T05:05:26Z

Affected Software/OS

The following products are know to use such weak credentials:

- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x

- CVE-2004-2357: Proofpoint Protection Server

- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6

- CVE-2007-2554: Associated Press (AP) Newspower 4.0.1 and earlier

- CVE-2007-6081: AdventNet EventLog Analyzer build 4030

- CVE-2009-0919: XAMPP

- CVE-2014-3419: Infoblox NetMRI before 6.8.5

- CVE-2015-4669: Xsuite 2.x

- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4

Other products might be affected as well.

Solution

Solution Type: Mitigation
- Change the password as soon as possible

- Contact the vendor for other possible fixes / updates

References

CVE CVE-2001-0645
CVE-2004-2357
CVE-2006-1451
CVE-2007-2554
CVE-2007-6081
CVE-2009-0919
CVE-2014-3419
CVE-2015-4669
CVE-2016-6531
CVE-2018-15719

Severity Rating: 10

What danger the CVE presents to the system

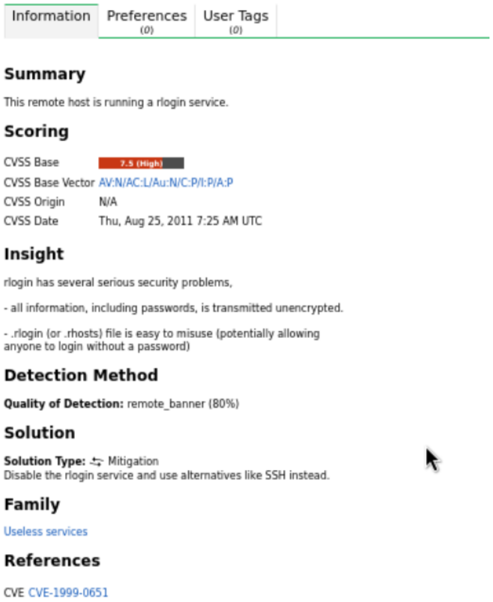
I could log into MySQL root user without a password, a critical misconfiguration. An attacker exploiting could gain unrestricted administrative access to the MySQL database and change, steal and add data.

What you did to fix it

The fix was changing the SQL password. Since it was an SQL 5.6 or earlier, I had to stop SQL service and then start MySQL safe mode in the background and log in without needing a password. From there, I logged into MySQL shell and updated the root password.

3. Rlog

CVE CVE-1999-0651



Summary

This remote host is running a rlogin service.

Scoring

CVSS Base 7.5 (High)
CVSS Base Vector AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Origin N/A
CVSS Date Thu, Aug 25, 2011 7:25 AM UTC

Insight

rlogin has several serious security problems,

- all information, including passwords, is transmitted unencrypted.

- .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)

Detection Method

Quality of Detection: remote_banner (80%)

Solution

Solution Type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Family

Useless services

References

CVE CVE-1999-0651

Severity Rating: 7.5

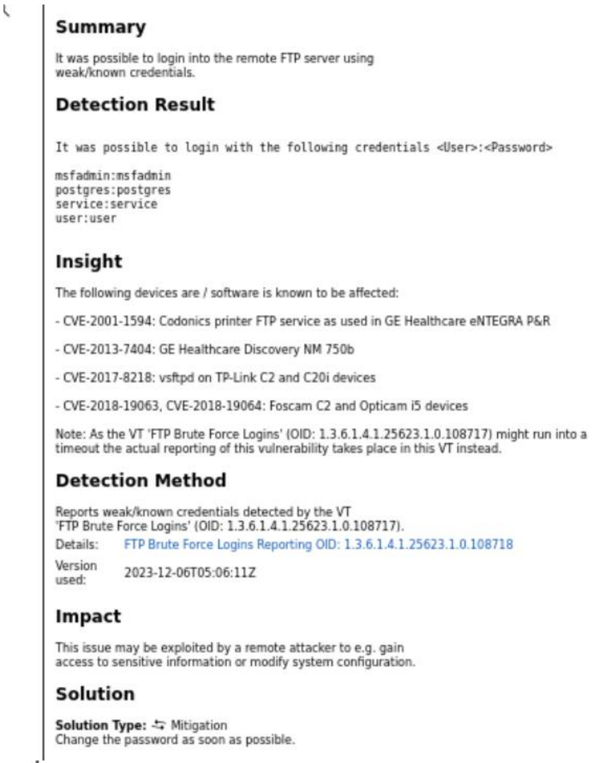
What danger the CVE presents to the system

This posed the same threat as rexec service by remote command execution on a host but uses unencrypted methods for authentication

What you did to fix it

I fixed it by sudo nano /etc/inetd.conf and disabled it by adding a # at the beginning of the rlogin service. Then, I enabled SSH service. And then, I rebooted the server. This makes sensitive credentials vulnerable to theft.

4. FTP
CVE CVE-1999-0501
CVE-1999-0502
CVE-1999-0507
CVE-1999-0508
CVE-2001-1594
CVE-2013-7404
CVE-2017-8218
CVE-2018-19063
CVE-2018-19064



Summary

It was possible to login into the remote FTP server using weak/known credentials.

Detection Result

```
It was possible to login with the following credentials <User>:<Password>

msfadmin:msfadmin
postgres:postgres
service:service
user:user
```

Insight

The following devices are / software is known to be affected:

- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R

- CVE-2013-7404: GE Healthcare Discovery NM 750b

- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices

- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Detection Method

Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).

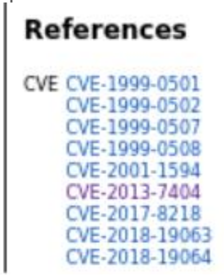
Details:	FTP Brute Force Logins Reporting OID: 1.3.6.1.4.1.25623.1.0.108718
Version used:	2023-12-06T05:06:11Z

Impact

This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution

Solution Type: ⇆ Mitigation
Change the password as soon as possible.



References

CVE CVE-1999-0501
CVE-1999-0502
CVE-1999-0507
CVE-1999-0508
CVE-2001-1594
CVE-2013-7404
CVE-2017-8218
CVE-2018-19063
CVE-2018-19064

Severity Rating: 7.5

What danger the CVE presents to the system

Allowing logins with weak or default credentials, such as msfadmin:msfadmin or postgres:postgres, enables attackers to easily gain unauthorized access. This can lead to severe consequences, including data breaches, system configuration modifications, and further exploitation of connected networks.

What you did to fix it

I fixed it by changing the password of msfadmin, postgres, service, and user to something strong and not easily guessable.

5. RSH
CVE CVE-1999-0651

Severity Rating: 7.5

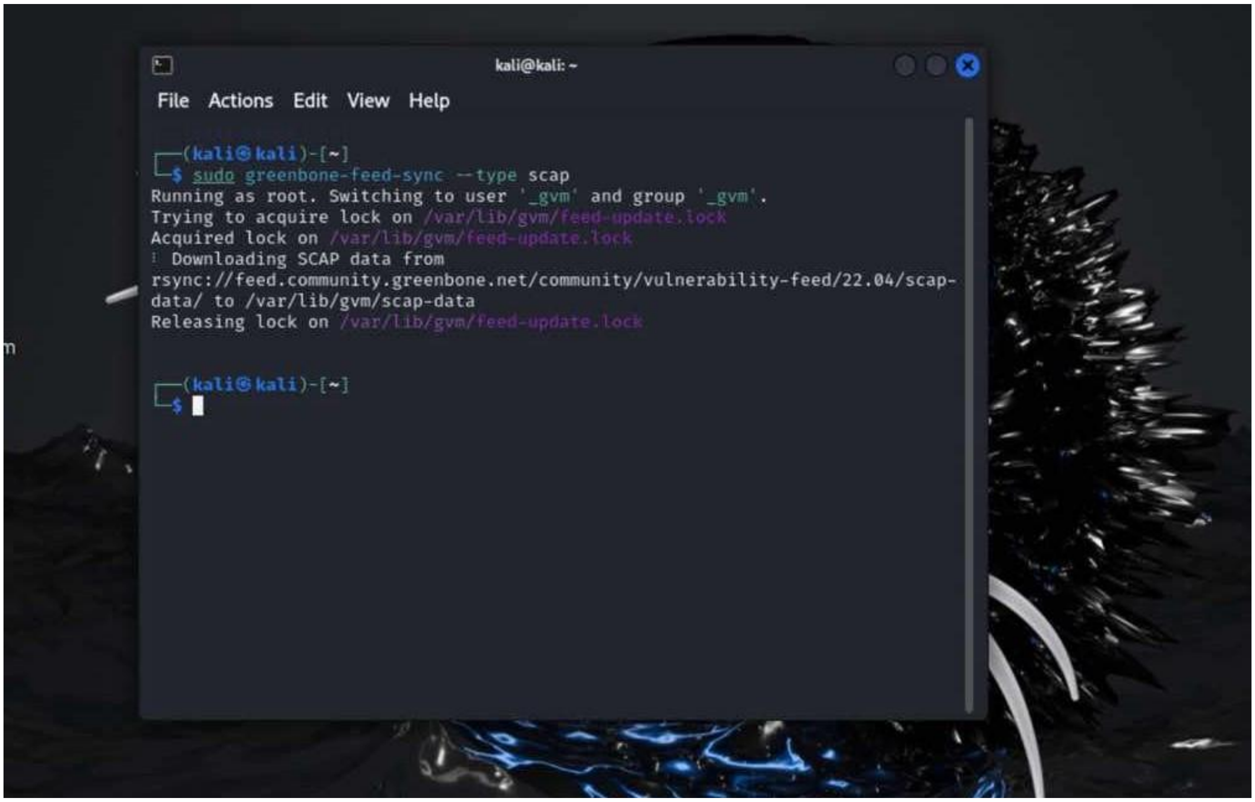
What danger the CVE presents to the system

This posed the same threat as rexec service by remote command execution on a host but uses unencrypted methods for authentication

What you did to fix it
I fixed it by sudo nano /etc/inetd.conf and disabled it by adding a # at the beginning of the rsh service. Then, I enabled SSH service. And then, I rebooted the server. This makes sensitive credentials vulnerable to theft.

Screenshots

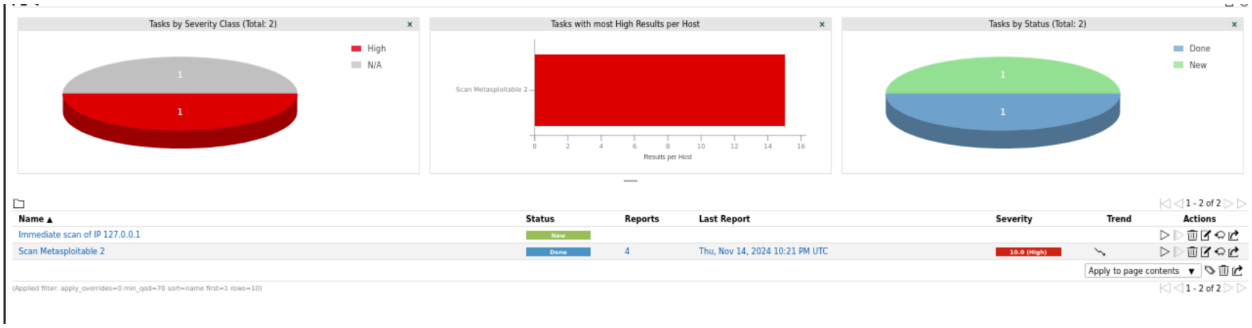
OpenVAS feeds have been synced



```
┌──(kali㉿kali)-[~]
└─$ sudo greenbone-feed-sync --type scap
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
⠸ Downloading SCAP data from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-
data/ to /var/lib/gvm/scap-data
Releasing lock on /var/lib/gvm/feed-update.lock

┌──(kali㉿kali)-[~]
└─$ 
```

Metasploitable 2 has been scanned



Tasks by Severity Class (Total: 2)
High
N/A
1
1
Tasks with most High Results per Host
Scan Metasploitable 2
0
2
4
6
8
10
12
14
16
Results per Host
Tasks by Status (Total: 2)
Done
New
1
1

1 - 2 of 2

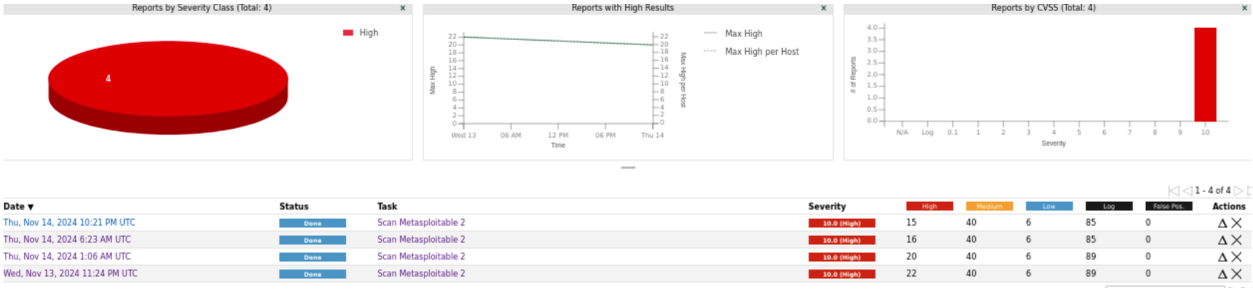
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 127.0.0.1	New					
Scan Metasploitable 2	Done	4	Thu, Nov 14, 2024 10:21 PM UTC	10.0 (High)	↘	

Apply to page contents ▾

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 2 of 2

Metasploitable 2 After Remediations



Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Thu, Nov 14, 2024 10:21 PM UTC	Done	Scan Metasploitable 2	10.0 (High)	15	40	6	85	0	Δ ✕
Thu, Nov 14, 2024 6:23 AM UTC	Done	Scan Metasploitable 2	10.0 (High)	16	40	6	85	0	Δ ✕
Thu, Nov 14, 2024 1:06 AM UTC	Done	Scan Metasploitable 2	10.0 (High)	20	40	6	89	0	Δ ✕
Wed, Nov 13, 2024 11:24 PM UTC	Done	Scan Metasploitable 2	10.0 (High)	22	40	6	89	0	Δ ✕