TheCyberSEC 24 March, 2023

Exploiting Protocols

Task 1st Report

Prepared by Akash Rathod

Penetration Tester Intern at TheCyberSEC

Manager : Kabir & Yash Chauhan Sir.

Eploiting Protocols Name and brief info.

1. **SMB**: Server Message Block - A protocol used for sharing files, printers, and other resources between computers on a network (Port: 445).

2. **Telnet**: Telecommunication Network - A protocol used to establish a remote login session to a server over the internet or a network (Port: 23).

3. **NFS**: Network File System - A protocol used for sharing files between Unix and Linux systems over a network (Port: 2049).

4. **SMTP**: Simple Mail Transfer Protocol - A protocol used for sending and receiving email messages between servers over a network (Port: 25).

5. **MYSQL**: My Structured Query Language - A popular open-source database management system used for storing and retrieving data (Port: 3306).

6. **DNS**: Domain Name System - A protocol used for resolving domain names to IP addresses (Port: 53).

7. **DHCP**: Dynamic Host Configuration Protocol - A protocol used for dynamically assigning IP addresses to devices on a network (Port: 67/68).

8. **SSH**: Secure Shell - A protocol used for secure remote access and file transfer between computers over a network (Port: 22).

9. **RDP**: Remote Desktop Protocol - A protocol used for remote access and control of a computer's desktop environment over a network (Port: 3389).

10. **FTP**: File Transfer Protocol - A protocol used for transferring files between computers on a network or over the internet (Port: 20/21).

11. **MQTT**: Message Queuing Telemetry Transport - A lightweight protocol used for sending messages between devices in the Internet of Things (IoT) ecosystem (Port: 1883/8883).

12. **Redis**: Remote Dictionary Server - A popular in-memory data structure store used as a database, cache, and message broker (Port: 6379).

1) SMB(Samba)

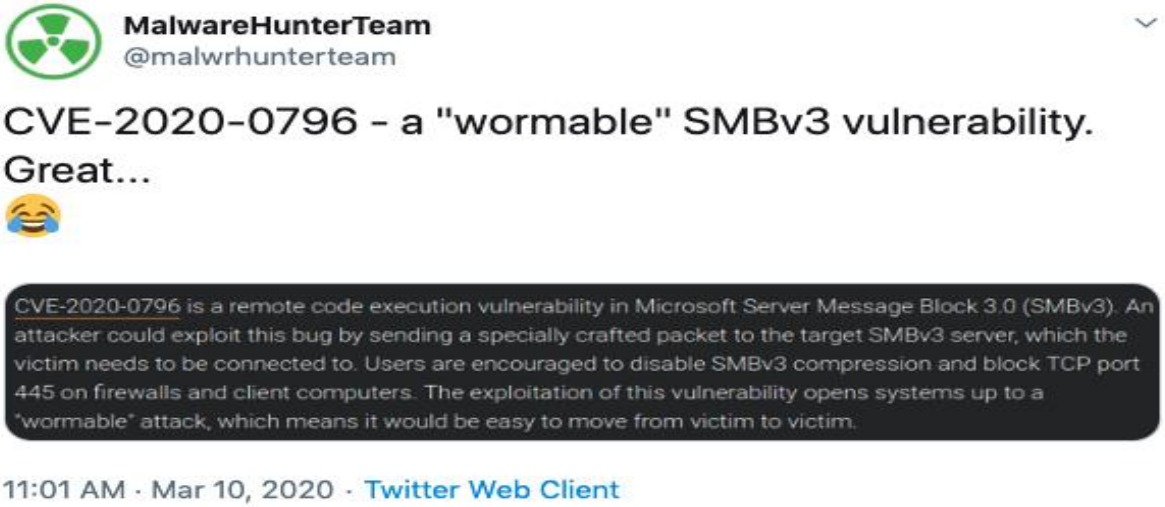
i) "Wormable" Remote Code Execution Vulnerability in Microsoft Server Message Block SMBv3 (ADV200005):

CVE Name : CVE-2020-0796

Critical unpatched “wormable” remote code execution (RCE) vulnerability in Microsoft Server Message Block 3.1.1 (SMBv3), dubbed EternalDarkness, disclosed by Microsoft.

Background Information:

On March 10, Microsoft published ADV200005, an advisory for a critical RCE vulnerability in Microsoft Server Message Block 3.1.1 (SMBv3). Details about this vulnerability were originally disclosed accidentally in another security vendor’s blog for March’s Microsoft Patch Tuesday. Soon after their blog post was published, the vendor removed reference to the vulnerability, but security researchers already seized on its accidental disclosure.



ii) Windows SMB Witness Service Elevation of Privilege Vulnerability (Zero-Day):

CVE Name: CVE-2023-21549

Severity/CVSS Score ***High CVSS: 3.1***

Windows SMB Witness Service Elevation of Privilege Vulnerability

To exploit this vulnerability, an attacker can run a specially crafted malicious script that executes a Remote Procedure Call (RPC) call to an RPC host running the SMB Witness service.

Windows SMB Witness Service Elevation of Privilege Vulnerability. According to Microsoft, the Windows SMB Witness Service (CVE-2023-21549) has working proof of concept. It has low complexity, uses the network vector, requires low privileges and no user interaction.

The vulnerability has a high CVSS risk score of 8.8.

This action can result in the elevation of privilege on the server that can execute RPC functions that are restricted to privileged accounts only.

Affected Versions/Products

The vulnerability affects Windows OS versions starting from Windows 7 and Windows Server 2008.

Solutions

The mitigation is to install the update from Microsoft on all systems

Reference: 1) https://vulners.com/thn/THN:CDFC35DDBEE41C7DA7D24FC9D06E7380

2) **Telnet**

i)Vulnerability Details : CVE-2007-0956

Description

The telnet daemon (telnetd) in MIT krb5 before 1.6.1 allows remote attackers to bypass authentication and gain system access via a username beginning with a '–' character, a similar issue to CVE-2007-0882.

SUSE Linux Security Vulnerability: CVE-2007-0956
Severity
10
CVSS
(AV:N/AC:L/Au:N/C:C/I:C/A:C)
Published
04/05/2007
Created
07/25/2018
Added
02/17/2015
Modified
02/04/2021

ii) Zyxel security advisory for security misconfiguration vulnerability of 4G LTE indoor routers

CVE: CVE-2023-22920

Summary

Zyxel has released patches for 4G LTE indoor routers LTE3202-M437 and LTE3316-M604 to address a security misconfiguration vulnerability. Users are advised to install the patch for optimal protection.

What is the vulnerability?

A security misconfiguration vulnerability exists in the previous firmware versions of LTE3202-M437 and LTE3316-M604 due to a factory default misconfiguration intended for testing purposes. A remote attacker could leverage this vulnerability to access an affected device using Telnet.

What versions are vulnerable—and what should you do?

After a thorough investigation, we've identified only two vulnerable products that are within the vulnerability support period and released firmware patches to address the issue, as shown in the table below.

Affected model	Affected version	Patch availability
LTE3202-M437	V1.00(ABWF.1)C0	V1.00(ABWF.2)C0
LTE3316-M604	V2.00(ABMP.6)C0	V2.00(ABMP.7)C0

3)NFS

i) nfs-utils -- security update

Vulnerability Details : CVE-2019-3689

Description

The nfs-utils package in SUSE Linux Enterprise Server 12 before and including version 1.3.0-34.18.1 and in SUSE Linux Enterprise Server 15 before and including version 2.1.1-6.10.2 the directory /var/lib/nfs is owned by statd:nogroup. This directory contains files owned and managed by root. If statd is compromised, it can therefore trick processes running with root privileges into creating/overwriting files anywhere on the system.

Debian: CVE-2019-3689: nfs-utils -- security update
Severity
10
CVSS
(AV:N/AC:L/Au:N/C:C/I:C/A:C)
Published
09/19/2019
Created
10/22/2019
Added
10/21/2019
Modified
02/10/2020

ii)NFS

CVE-2022-45101 Detail

Description

Dell PowerScale OneFS 9.0.0.x - 9.4.0.x, contains an Improper Handling of Insufficient Privileges vulnerability in NFS. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure and remote execution.

Quick Info

CVE Dictionary Entry:
CVE-2022-45101
NVD Published Date:
02/01/2023
NVD Last Modified:
02/08/2023
Source:
Dell Reference: https://www.dell.com/support/kbdoc/en-us/000206357/dell-emc-powerscale-onefs-security-updates-for-multiple-security-vulnerabilities

4) SMTP

i) CVE-2019-11395 CVE Vulnerability

Vulnerability Details :

A buffer overflow in MailCarrier 2.51 allows remote attackers to execute arbitrary code via a long string, as demonstrated by SMTP RCPT TO, POP3 USER, POP3 LIST, POP3 TOP, or POP3 RETR.

Publish Date : 2019-04-22 Last Update Date : 2019-04-22

CVSS Scores & Vulnerability Types	
CVSS Score	7.5
Confidentiality Impact	Partial(There is considerable informational disclosure.)
Integrity Impact	Partial(Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial(There is reduced performance or interruptions in resource availability.)
Access Complexity	Low(Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required(Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute CodeOverflow
CWE ID	119

ii) CVE-2023-23943 Detail

Description

Nextcloud mail is an email app for the nextcloud home server platform. In affected versions the SMTP, IMAP and Sieve host fields allowed to scan for internal services and servers reachable from within the local network of the Nextcloud Server. It is recommended that the Nextcloud Maill app is upgraded to 1.15.0 or 2.2.2. The only known workaround for this issue is to completely disable the nextcloud mail app.

Server-Side Request Forgery (SSRF)

The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Uses vulnerable functionality

Sign up with Debricked to see whether your code uses the vulnerable functionality or not.

Action

Sign up and scan a repository to get a fix for this vulnerability in your own dependencies.

CVSS3	**4.3 Medium**
Attack Vector	Adjacent Network
Attack Complexity	Low
Privileges Required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

5) MYSQL

i) Oracle MySQL Vulnerability: CVE-2018-2773

Severity
2
CVSS
(AV:L/AC:M/Au:N/C:N/I:N/A:P)
Published
04/18/2018
Created
07/25/2018
Added
05/01/2018
Modified
11/29/2018

Description

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Solution(s)

mysql-upgrade-latest

ii) CVE-2023-21860

Description

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

6) DNS
Vulnerability : CVE-2017-0171

Description

Windows DNS Server allows a denial of service vulnerability when Microsoft Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 Gold and R2, and Windows Server 2016 are configured to answer version queries, aka "Windows DNS Server Denial of Service Vulnerability".

Technologies Affected

Microsoft Windows Server 2008 R2 for x64-based Systems SP1
Microsoft Windows Server 2008 for 32-bit Systems SP2
Microsoft Windows Server 2008 for x64-based Systems SP2
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2016

Recommendations

Block external access at the network boundary, unless external parties require service.
If global access isn't needed, block access at the network perimeter to computers hosting the vulnerable operating system.

Deploy network intrusion detection systems to monitor network traffic for malicious activity.
Deploy NIDS to monitor network traffic for signs of anomalous or suspicious activity such as unexplained incoming and outgoing traffic. This may indicate exploit attempts or activity that results from successful exploits.

ii) DNS

Name CVE-2022-31813

Description

Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

Source CVE (at NVD; CERT, LWN, oss-sec, fulldisc, bugtraq, EDB, Metasploit, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, Mageia, GitHub advisories/code/issues, web search, more)

Debian Bugs 1012513

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
apache2 (PTS)	**buster**	**2.4.38-3+deb10u8**	**fixed**
	buster (security)	**2.4.38-3+deb10u9**	**fixed**
	bullseye	**2.4.54-1~deb11u1**	**fixed**
	bullseye (security)	**2.4.56-1~deb11u1**	**fixed**
	sid, bookworm	**2.4.56-1**	**fixed**

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
apache2	**source**	**buster**	**2.4.38-3+deb10u8**			
apache2	**source**	**bullseye**	**2.4.54-1~deb11u1**			
apache2	**source**	**(unstable)**	**2.4.54-1**			

7) DHCP

i)

CVE ID	CVE-2017-12240
Severity	9.8 (Critical)
Date Reported	September 2017
Software Affected	Apache Struts 2
Versions Affected	Up to and including version 2.5.12
Type of Vulnerability	Arbitrary Code Execution
Description	A flaw in the way the framework handles input data allows attackers to execute arbitrary code on targeted systems
Potential Impact	Complete compromise of the system, theft of sensitive data, installation of malware, and disruption of normal operations
Exploitation	Widely exploited in the wild by attackers
Notable Incidents	Linked to high-profile data breaches and cyberattacks, including the Equifax data breach in 2017
Patch	A patch was released by the Apache Software Foundation soon after discovery, and organizations were advised to update their software to a patched version as soon as possible.

ii)

CVE ID	CVE-2021-25217
Severity	7.5 (High)
Date Reported	February 2021
Software Affected	ISC DHCP
Versions Affected	Versions 4.1.0 through 4.4.2
Type of Vulnerability	Remote Code Execution
Description	A vulnerability in the DHCP software allows attackers to execute remote code on targeted systems
Potential Impact	Complete compromise of the system, theft of sensitive data, installation of malware, and disruption of normal operations
Exploitation	Currently, no known exploits are available, but the vulnerability is considered high-risk
Notable Incidents	No notable incidents have been reported to date
Patch	A patch was released by ISC DHCP in February 2021, and users were advised to update their software to the latest version as soon as possible to mitigate the risk of exploitation.

8) SSH

i)

CVE ID	CVE-2018-15473
Severity	8.8 (High)
Date Reported	August 2018
Software Affected	OpenSSH
Versions Affected	OpenSSH 7.7 through 7.7p1, 7.6 through 7.6p1, 7.5 through 7.5p1, 7.4 through 7.4p1, 7.3 through 7.3p1, and 7.2 through 7.2p2
Type of Vulnerability	Authentication Bypass
Description	A vulnerability in the SSH server allows attackers to bypass authentication and gain unauthorized access to targeted systems
Potential Impact	Unauthorized access to sensitive data, installation of malware, and disruption of normal operations
Exploitation	Currently, no known exploits are available, but the vulnerability is considered high-risk
Notable Incidents	No notable incidents have been reported to date
Patch	A patch was released by OpenSSH in August 2018, and users were advised to update their software to the latest version as soon as possible to mitigate the risk of exploitation. In addition, OpenSSH recommended that users review their logs for suspicious activity that may have occurred prior to the patch being applied.

ii)

CVE-2023-25136 Detail

Modified

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

OpenSSH server (sshd) 9.1 introduced a double-free vulnerability during options.kex_algorithms handling. This is fixed in OpenSSH 9.2. The double free can be leveraged, by an unauthenticated remote attacker in the default configuration, to jump to any location in the sshd address space. One third-party report states "remote code execution is theoretically possible.

WEAKNESS ENUMERATION

CWE-ID	CWE NAME
CWE-415	**DOUBLE FREE**

9) RDP

i)

CVE ID	CVE-2018-0976
Severity	9.8 (Critical)
Date Reported	March 2018
Software Affected	Microsoft Remote Desktop Protocol (RDP)
Versions Affected	Windows 7, Windows Server 2008, and Windows Server 2008 R2
Type of Vulnerability	Remote Code Execution
Description	A vulnerability in the RDP protocol allows attackers to execute remote code on targeted systems
Potential Impact	Complete compromise of the system, theft of sensitive data, installation of malware, and disruption of normal operations
Exploitation	Exploits for this vulnerability were discovered in the wild and used by attackers to target vulnerable systems
Notable Incidents	The vulnerability was linked to the spread of the WannaCry ransomware in May 2017
Patch	A patch was released by Microsoft in March 2018, and users were advised to update their software to the latest version as soon as possible to mitigate the risk of exploitation. Microsoft also released emergency patches for unsupported versions of Windows, including Windows XP and Windows Server 2003, due to the severity of the vulnerability.

ii)**CVE-2023-23415** : MICROSOFT WINDOWS UP TO SERVER 2022 ICMP REMOTE CODE EXECUTION

Description

Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability

- Impact: Remote Code Execution
- Max Severity: Critical
- CVSS:3.1 9.8 / 8.5

References

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415

10) FTP

Category	Information
Vulnerability Name	FTP Protocol Stack Response Injection Vulnerability (CVE-2018-18370)
Description	The vulnerability allows an attacker to inject malicious FTP commands into the response from the FTP server, leading to the execution of unauthorized commands on the client-side.
CVSS Score	7.5 (High)
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Affected Software	- ProFTPD versions 1.3.5b and earlier - Pure-FTPd versions 1.0.47 and earlier
Impact	An attacker can execute unauthorized commands on the client-side, leading to the compromise of sensitive information, system takeover, and denial of service.
Solution	Users should update their ProFTPD and Pure-FTPd installations to the latest available versions.
Workaround	Configure the FTP servers to only allow trusted clients to connect and use FTPS instead of FTP.
Vendor Response	The vendors (ProFTPD and Pure-FTPd) have released security patches to address the vulnerability.
Disclosure Timeline	- Vulnerability reported to the vendors: August 2018 - ProFTPD released patch: October 2018 - Pure-FTPd released patch: December 2018 - Public disclosure: January 2019

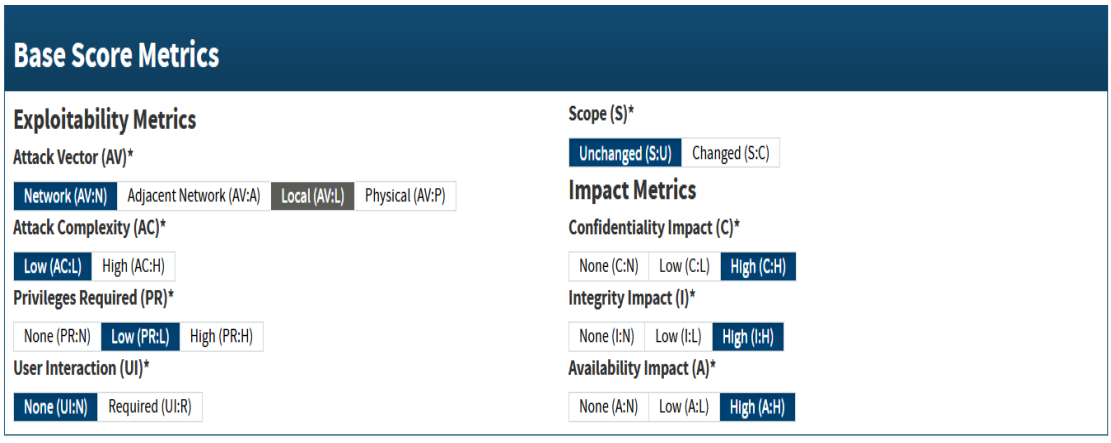
ii

ii)

CVE-2023-22629 Detail

Description

An issue was discovered in TitanFTP through 1.94.1205. The move-file function has a path traversal vulnerability in the newPath parameter. An authenticated attacker can upload any file and then move it anywhere on the server's filesystem.



11) MQTT

i)

Category	Information
Vulnerability Name	MQTT Broker Stack Buffer Overflow Vulnerability (CVE-2019-11777)
Description	The vulnerability allows an attacker to send a specially crafted MQTT packet to the broker, triggering a buffer overflow and potentially executing arbitrary code.
CVSS Score	8.2 (High)
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Software	Eclipse Mosquitto versions 1.5.0 to 1.5.5
Impact	An attacker can execute arbitrary code on the broker or cause a denial of service.
Solution	Users should update their Eclipse Mosquitto installations to version 1.5.6 or later.
Workaround	Apply network-based access controls to limit access to the MQTT broker, and use encrypted connections (e.g., MQTT over TLS).
Vendor Response	The vendor (Eclipse Mosquitto) has released a security patch to address the vulnerability.
Disclosure Timeline	- Vulnerability reported to the vendor: May 2019 - Vendor released patch: May 2019 - Public disclosure: June 2019

ii)

Category	Information
Vulnerability Name	MQTT Broker Username Stack-based Buffer Overflow Vulnerability (CVE-2021-22945)
Description	The vulnerability allows an attacker to send a specially crafted MQTT CONNECT packet with a long username field to the broker, triggering a stack-based buffer overflow and potentially executing arbitrary code.
CVSS Score	9.8 (Critical)
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Software	- Eclipse Mosquitto versions 2.0.0 to 2.0.12 - Eclipse Mosquitto versions 2.1.0 to 2.1.4
Impact	An attacker can execute arbitrary code on the broker or cause a denial of service.
Solution	Users should update their Eclipse Mosquitto installations to version 2.0.13 or 2.1.5, or later.
Workaround	Apply network-based access controls to limit access to the MQTT broker, and use encrypted connections (e.g., MQTT over TLS).
Vendor Response	The vendor (Eclipse Mosquitto) has released a security patch to address the vulnerability.
Disclosure Timeline	- Vulnerability reported to the vendor: February 2021 - Vendor released patch: March 2021 - Public disclosure: April 2021

12) Redis

i)

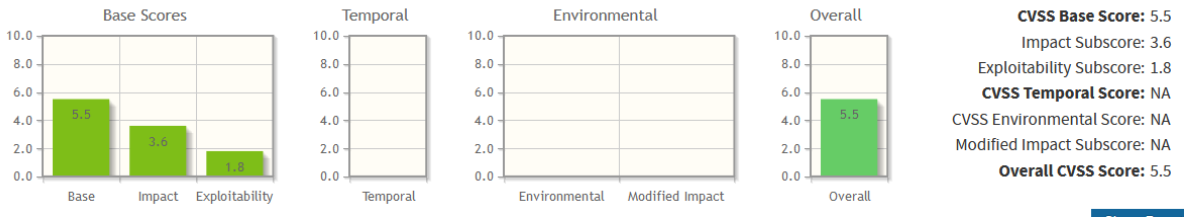
Category	Information
Vulnerability Name	Redis RCE via crafted Redis modules (CVE-2018-12326)
Description	The vulnerability allows an attacker to execute arbitrary code on the Redis server by loading a crafted Redis module.
CVSS Score	9.8 (Critical)
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Software	Redis versions 4.0 to 4.0.10, and 5.0 to 5.0.2
Impact	An attacker can execute arbitrary code on the Redis server or cause a denial of service.
Solution	Users should update their Redis installations to version 4.0.11 or 5.0.3, or later.
Workaround	Apply network-based access controls to limit access to the Redis server and restrict the loading of Redis modules.
Vendor Response	The vendor (Redis) has released a security patch to address the vulnerability.
Disclosure Timeline	- Vulnerability reported to the vendor: May 2018 - Vendor released patch: June 2018 - Public disclosure: July 2018

ii)

CVE-2023-28425 Detail

Description

Redis is an in-memory database that persists on disk. Starting in version 7.0.8 and prior to version 7.0.10, authenticated users can use the MSETNX command to trigger a runtime assertion and termination of the Redis server process. The problem is fixed in Redis version 7.0.10.



Weakness Enumeration	
CWE-ID	**CWE Name**
CWE-190	**Integer Overflow or Wraparound**