

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures (CVE) Report

16 - 29 Feb 2024

Vol. 11 No. 04

Table of Content								
Vendor	Product	Page Number						
Application								
Apache	commons_compress	1						
connectwise	screenconnect	2						
Gitlab	gitlab	3						
Intel	inet_wireless_daemon	13						
Oracle	mysql_server	13						
W1.fi	wpa_supplicant	24						
Operating System								
Cisco	nx-os	25						
Debian	debian_linux	350						
Fedoraproject	fedora	351						
Google	android	352						
avogie	chrome_os	352						
Linux	linux_kernel	353						
Redhat	enterprise_linux	354						

Common Vulnerabilities and Exposures (CVE) Report								
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
		<u> </u>	Application					
Vendor: Apa	ache							
Product: co	mmons_compi	ess						
Affected Ver	sion(s): From (i	ncluding)	1.21.0 Up to (excludin	ng) 1.26.0	1			
Allocation of Resources Without Limits or Throttling	19-Feb-2024	5.5	Allocation of Resources Without Limits or Throttling vulnerability in Apache Commons Compress. This issue affects Apache Commons Compress: from 1.21 before 1.26. Users are recommended to upgrade to version 1.26, which fixes the issue. CVE ID : CVE- 2024-26308	https://lists.apa che.org/thread/ ch5yo2d21p7vl qrhll9b17otbyq 4npfg	A-APA-COMM- 070324/1			
Affected Ver	sion(s): From (i	ncluding)	1.3 Up to (excluding)	1.26.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	19-Feb-2024	5.5	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Apache Commons Compress.This issue affects Apache Commons Compress: from 1.3 through 1.25.0. Users are recommended to upgrade to version 1.26.0 which fixes the issue.	https://lists.apa che.org/thread/ cz8qkcwphy4cx 8gltn932ln51cb tq6kf	A-APA-COMM- 070324/2			

0-1

1-2

2-3

3-4 4-5 Page **1** of **356** 5-6

6-7

7-8

8-9

nectwise eenconnect ion(s): * Up to	(excludinį	ConnectWise		
eenconnect	(excludin	ConnectWise		
	(excludins	ConnectWise		
i <mark>on(s): * Up to</mark>	(excludinį	ConnectWise		
21-Feb-2024	8.4	ScreenConnect 23.9.7 and prior are affected by path-traversal vulnerability, which may allow an attacker the ability to execute remote code or directly impact confidential data or critical systems.	https://www.co nnectwise.com/ company/trust/ security- bulletins/conne ctwise- screenconnect- 23.9.8	A-CON-SCRE- 070324/3
21-Feb-2024	10	ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems. CVE ID : CVE- 2024-1709	https://www.co nnectwise.com/ company/trust/ security- bulletins/conne ctwise- screenconnect- 23.9.8	A-CON-SCRE- 070324/4
		21-Feb-2024 10	21-Feb-20248.4the ability to execute remote code or directly impact confidential data or critical systems.21-Feb-20240CVE ID : CVE- 2024-170821-Feb-202410ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.21-Feb-202410	21-Feb-20248.4the ability to execute remote code or directly impact confidential data or critical systems.security- bulletins/conne ctwise- screenconnect- 23.9.821-Feb-202410CVE ID : CVE- 2024-1708Impact Confidential data or critical systems.21-Feb-202410ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channelhttps://www.co nnectwise.com/ company/trust/ security- bulletins/conne ctwise- screenconnect- 23.9.821-Feb-202410Vulnerability, which may allow an attacker direct access to confidential information or critical systems.https://www.co nnectwise- screenconnect- 23.9.8

Page **2** of **356**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Gitl	ab	I		L	
Product: git	lab				
Affected Vers	sion(s): * Up to	(including	g) 16.7.6		
N/A	21-Feb-2024	5.4	An issue has been discovered in GitLab affecting all versions before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. It was possible for group members with sub- maintainer role to change the title of privately accessible deploy keys associated with projects in the group. CVE ID : CVE- 2023-3509	N/A	A-GIT-GITL- 070324/5
Affected Vers	sion(s): 16.9.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2024	8.7	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.9 before 16.9.1. A crafted payload added to the user profile page could lead to a stored XSS on the client side, allowing attackers to perform arbitrary actions on behalf of victims."	N/A	A-GIT-GITL- 070324/6
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 74	-8 8-9 9-10
CVSS Scoring S	ocale 0-1	1-2 2	- 3 3-4 4-5 Page 3 of 356	5-6 <u>6</u> -7 7	-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-1451		
N/A	22-Feb-2024	7.7	An authorization bypass vulnerability was discovered in GitLab affecting versions 15.1 prior to 16.7.6, 16.8 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge conflict. CVE ID : CVE- 2024-0410	N/A	A-GIT-GITL- 070324/7
N/A	22-Feb-2024	6.7	An issue has been discovered in GitLab EE affecting all versions starting from 16.5 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. When a user is assigned a custom role with admin_group_mem ber permission, they may be able to make a group, other members or themselves Owners of that group, which may lead to privilege escalation.	N/A	A-GIT-GITL- 070324/8

0-1

1-2

2-3

3-4 4-5 Page **4** of **356** 8-9

9-10

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2023-6477		
N/A	21-Feb-2024	5.4	An issue has been discovered in GitLab affecting all versions before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. It was possible for group members with sub- maintainer role to change the title of privately accessible deploy keys associated with projects in the group. CVE ID : CVE- 2023-3509	N/A	A-GIT-GITL- 070324/9
N/A	22-Feb-2024	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Under some specialized conditions, an LDAP user may be able to reset their password using their verified secondary email address and sign-in	N/A	A-GIT-GITL- 070324/10

0-1

1-2

2-3

3-4 4-5 Page **5** of **356** 6-7 7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using direct authentication with the reset password, bypassing LDAP. CVE ID : CVE- 2024-1525		
N/A	22-Feb-2024	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 16.4 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Users with the `Guest` role can change `Custom dashboard projects` settings contrary to permissions. CVE ID : CVE- 2024-0861	N/A	A-GIT-GITL- 070324/11
N/A	22-Feb-2024	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 to 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. This vulnerability allows for bypassing the 'group ip restriction' settings to access	N/A	A-GIT-GITL- 070324/12

Page **6** of **356**

N/A22-Feb-20247.77.7An authorization bypass by assing the 'group ip restriction's ettings to access environment details of projects CVE ID : CVE- 2023-4895N/AA-GIT-GITL- 070324/14N/A22-Feb-20247.7An authorization bypass vulnerability was discovered in GitLab affecting versions 15.1 prior to 16.8.3, and 16.9 prior to 16.8.3, and 16.9 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge conflict.N/AA-GIT-GITL- 070324/14	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A22-Feb-2024An issue has been discovered in GitLab EE affecting all versions starting from 12.0 to 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1.This vulnerability allows for bypassing the 'group ip restriction' settings to access environment details of projectsN/AA-GIT-GITL- 070324/13Affected Version(s): From (including)15.1.0 Up to (excluding) 16.7.6N/AA-GIT-GITL- 070324/13N/A22-Feb-20247.7An authorization bypass vulnerability was discovered in GitLab affecting versions 15.1 prior to 16.7.6, 16.8 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass (ODEOWNERS approvals by creating a merge conflict.N/AA-GIT-GITL- 070324/14				details of projects CVE ID : CVE-		
N/A22-Feb-20244.3discovered in GitLab EE affecting all versions starting from 12.0 	Affected Ver	sion(s): From (i	ncluding)	12.0 Up to (including)) 16.76	
N/A 22-Feb-2024 7.7 Prior to 16.8.3, and 16.9 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge conflict.	N/A	22-Feb-2024	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 to 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. This vulnerability allows for bypassing the 'group ip restriction' settings to access environment details of projects CVE ID : CVE- 2023-4895	N/A	
N/A 22-Feb-2024 7.7 by prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge conflict.	Affected Ver	sion(s): From (i	ncluding)		ng) 16.7.6	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	N/A	22-Feb-2024	7.7	bypass vulnerability was discovered in GitLab affecting versions 15.1 prior to 16.7.6, 16.8 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge	N/A	
	CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	<u> </u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-0410		
Affected Ver	sion(s): From (i	ncluding)	16.1 Up to (excluding) 16.7.6	
N/A	22-Feb-2024	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Under some specialized conditions, an LDAP user may be able to reset their password using their verified secondary email address and sign-in using direct authentication with the reset password, bypassing LDAP. CVE ID : CVE- 2024-1525	N/A	A-GIT-GITL- 070324/15
Affected Ver	sion(s): From (i	ncluding)	16.4.0 Up to (excludin	ng) 16.7.6	
N/A	22-Feb-2024	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 16.4 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Users with the	N/A	A-GIT-GITL- 070324/16

0-1

1-2

2-3

3-4 4-5 Page **8** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`Guest` role can change `Custom dashboard projects` settings contrary to permissions. CVE ID : CVE-		
			2024-0861		
Affected Ver	sion(s): From (i	ncluding)	16.5.0 Up to (excludir	ng) 16.7.6	1
N/A	22-Feb-2024	6.7	An issue has been discovered in GitLab EE affecting all versions starting from 16.5 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. When a user is assigned a custom role with admin_group_mem ber permission, they may be able to make a group, other members or themselves Owners of that group, which may lead to privilege escalation. CVE ID : CVE- 2023-6477	N/A	A-GIT-GITL- 070324/17
Affected Ver	sion(s): From (i	ncluding)	16.8 Up to (excluding) 16.8.3	
N/A	22-Feb-2024	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before	N/A	A-GIT-GITL- 070324/18

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Under some specialized conditions, an LDAP user may be able to reset their password using their verified secondary email address and sign-in using direct authentication with the reset password, bypassing LDAP. CVE ID : CVE- 2024-1525		
N/A	22-Feb-2024	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.0 to 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. This vulnerability allows for bypassing the 'group ip restriction' settings to access environment details of projects CVE ID : CVE- 2023-4895	N/A	A-GIT-GITL- 070324/19

0-1

1-2

2-3

3-4 4-5 Page **10** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Feb-2024	7.7	An authorization bypass vulnerability was discovered in GitLab affecting versions 15.1 prior to 16.7.6, 16.8 prior to 16.8.3, and 16.9 prior to 16.9.1. A developer could bypass CODEOWNERS approvals by creating a merge conflict. CVE ID : CVE-	N/A	A-GIT-GITL- 070324/20
			2024-0410		
N/A	22-Feb-2024	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 16.4 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. Users with the `Guest` role can change `Custom dashboard projects` settings contrary to permissions. CVE ID : CVE- 2024-0861	N/A	A-GIT-GITL- 070324/21
Affected Ver	sion(s): From (i	ncluding)	16.8.0 Up to (includin	ı <mark>g) 16.8.3</mark>	
N/A	22-Feb-2024	6.7	An issue has been discovered in GitLab EE affecting all versions	N/A	A-GIT-GITL- 070324/22

0-1

1-2

2-3

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			starting from 16.5 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. When a user is assigned a custom role with admin_group_mem ber permission, they may be able to make a group, other members or themselves Owners of that group, which may lead to privilege escalation. CVE ID : CVE- 2023-6477		
N/A	21-Feb-2024	5.4	An issue has been discovered in GitLab affecting all versions before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. It was possible for group members with sub- maintainer role to change the title of privately accessible deploy keys associated with projects in the group. CVE ID : CVE- 2023-3509	N/A	A-GIT-GITL- 070324/23

0-1

1-2

2-3

3-4 4-5 Page **12** of **356** 5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Int	el	1	L	L	L
Product: ine	et_wireless_da	emon			
Affected Ver	sion(s): * Up to	(excludin	g) 2.14		
Improper Authentica tion	22-Feb-2024	7.5	The Access Point functionality in eapol_auth_key_ha ndle in eapol.c in iNet wireless daemon (IWD) before 2.14 allows attackers to gain unauthorized access to a protected Wi-Fi network. An attacker can complete the EAPOL handshake by skipping Msg2/4 and instead sending Msg4/4 with an all- zero key. CVE ID : CVE- 2023-52161	https://git.kern el.org/pub/scm /network/wirel ess/iwd.git/co mmit/?id=6415 420f1c92012f6 4063c131480ff cef58e60ca	A-INT-INET- 070324/24
Vendor: Ora	acle				
Product: my	ysql_server				
Affected Ver	sion(s): 8.1.0				
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/25

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H).		
N/A	17-Feb-2024	4.9	2024-20972 Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/26

0-1

1-2

2-3

3-4 4-5 Page **14** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20974		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/27

0-1

1-2

2-3

3-4 4-5 Page **15** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20976		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/28

0-1

1-2

2-3

3-4 4-5 Page **16** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20978		
Affected Ver	sion(s): 8.2.0		· · · · · · · · · · · · · · · · · · ·		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-0RA-MYSQ- 070324/29

0-1

1-2

2-3

3-4 4-5 Page **17** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20972		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/30

0-1

1-2

2-3

3-4 4-5 Page **18** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H).		
			CVE ID : CVE- 2024-20974		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/31

0-1

1-2

2-3

3-4 4-5

8-9 7-8 9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20976		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20978	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/32

0-1

1-2

2-3

3-4 4-5 Page **20** of **356** 5-6

6-7

7-8 8-9

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.35							
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20972	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/33		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle	https://www.or acle.com/securi ty-	A-ORA-MYSQ- 070324/34		

0-1

1-2

2-3

5-6

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20974	alerts/cpujan20 24.html	
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/35

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H). CVE ID : CVE- 2024-20976		
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily	https://www.or acle.com/securi ty- alerts/cpujan20 24.html	A-ORA-MYSQ- 070324/36

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows high privileged attacker with network access via multiple protocols 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 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A C:L/PR:H/UI:N/S:U /C:N/I:N/A:H).		
Vendor: W1	fi		2024-20978		
Product: wp	oa_supplicant				
Affected Ver	sion(s): * Up to	(excluding	g) 2.10		
Improper Authentica tion	22-Feb-2024	6.5	The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured	https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 e55255a81270 b768439c	A-W1WPA 070324/37

0-1

1-2

2-3

3-4 4-5 Page **24** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks. CVE ID : CVE- 2023-52160		
Vendor: Cis	60		Operating System		
Product: nx					
Affected Ver	sion(s): 10.1\\([1\\]			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/38

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network traffic or to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS) condition.		
			Note: The IPv6 packet can be		
			generated multiple		
			hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device processes the		
			processes the packet.		
			CVE ID : CVE-		
			2024-20267		
Allocation			A vulnerability in	https://sec.clou	
of	29-Feb-2024	8.6	the External	dapps.cisco.com	O-CIS-NX-O-
Resources		0.0	Border Gateway	/security/cente	070324/39
Without			Protocol (eBGP)	r/content/Cisco	

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Limits or Throttling			implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.	SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ				
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321					
Affected Ver	Affected Version(s): 10.1\\(2\\)							
Buffer Copy without Checking	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco	0-CIS-NX-0- 070324/40			

0-1

1-2

2-3

5-6

6-7

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	packet.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/41
			exploit could allow the attacker to cause eBGP		

0-1

1-2

2-3

3-4 4-5 Page **29** of **356** 5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			neighbor sessions to be dropped, leading to a DoS condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.1\\([2t\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-O- 070324/42

0-1

1-2

2-3

3-4 4-5 Page **30** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/43
			exists because eBGP traffic is mapped to a shared hardware		

0-1

1-2

2-3

3-4 4-5 Page **31** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	 <mark>sion(s): 10.2\\(</mark>	1\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/44
			This vulnerability is due to lack of		

0-1

1-2

2-3

3-4 4-5 Page **32** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-	O-CIS-NX-O- 070324/45

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Weakness	Publish Date	CVSSv3	Description & CVE ID allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network.	Patch nxos-ebgp-dos- L3QCwVJ	NCIIPC ID		
			CVE ID : CVE- 2024-20321				
Affected Ver	Affected Version(s): 10.2\\(1q\\)						
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated,	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/46		

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			remote attacker to	mpls-dos-	
Overflow')			cause the netstack	R9ycXkwM	
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **35** of **356** 5-6

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occur when the NX- OS device processes the packet. CVE ID : CVE-		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	2024-20267 A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/47

0-1

1-2

2-3

3-4 4-5 Page **36** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.2\\(2\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/48

0-1

1-2

2-3

3-4 4-5 Page **37** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/49

0-1

1-2

2-3

3-4 4-5 Page **38** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.2\\([3\\]			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/50

0-1

1-2

2-3

3-4 4-5 Page **39** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/51

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.2\\(3t\\)		I	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/52

0-1

1-2

3-4 4-5 Page **41** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-3

3-4 4-5 Page **42** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/53

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.2\\([3v\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/54

0-1

1-2

2-3

3-4 4-5 Page **44** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/55

0-1

1-2

2-3

3-4 4-5 Page **45** of **356** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.2\\(4\\)	<u> </u>	I	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/56

0-1

1-2

2-3

3-4 4-5 Page **46** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/57

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.2\\(5\\)		[
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/58

0-1

1-2

3-4 4-5 Page **48** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-3

3-4 4-5 Page **49** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/59

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.2\\(6\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/60

0-1

1-2

2-3

3-4 4-5 Page **51** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/61

0-1

1-2

2-3

3-4 4-5 Page **52** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.3\\(1\\)		<u> </u>	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/62

0-1

1-2

2-3

3-4 4-5 Page **53** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/63

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.3\\(2\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/64

0-1

1-2

3-4 4-5 Page **55** of **356** 5-6

6-7

2-3

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-3

3-4 4-5 Page **56** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/65

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.3\\([3\\]	-	-	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/66

0-1

1-2

2-3

3-4 4-5 Page **58** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/67

0-1

1-2

2-3

3-4 4-5 Page **59** of **356** 6-7

7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.3\\(4a\\)			
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/68

0-1

1-2

2-3

3-4 4-5 Page **60** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.3\\(99w\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/69

0-1

1-2

2-3

3-4 4-5 Page **61** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/70

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.3\\(99x\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/71

0-1

1-2

3-4 4-5 Page **63** of **356** 5-6

6-7

7-8

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-3

3-4 4-5 Page **64** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/72

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 10.4\\(1\\)		-	_
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/73

0-1

1-2

2-3

3-4 4-5 Page **66** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/74

0-1

1-2

2-3

3-4 4-5 Page **67** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 6.0\\(2	\\)a3\\(1	(/)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/75

0-1

1-2

2-3

3-4 4-5 Page **68** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a3\\(2	2\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/76

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from the targeted device		
			and then		
			encapsulated within MPLS. The		
			DoS condition may		
			occur when the NX-		

0-1

1-2

2-3

3-4 4-5 Page **70** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	/\\)a3\\(4	ł//)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/77

0-1

1-2

2-3

3-4 4-5 Page **71** of **356** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a4\\(1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/78
			This vulnerability is due to lack of proper error		

0-1

1-2

2-3

3-4 4-5 Page **72** of **356** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a4\\(2	2\\)		
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/79

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **74** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	2\\)a4\\(3	3\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/80

0-1

1-2

2-3

3-4 4-5 Page **75** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a4\\(4	ł//)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/81

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.0\\(2	:\\)a4\\(5		1	<u>'</u>
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	O-CIS-NX-O- 070324/82

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
L	I		0	I	<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **78** of **356** 5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	:\\)a4\\((
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/83

0-1

1-2

2-3

3-4 4-5 Page **79** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(1	2024-20267		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/84

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			network traffic or				
			to reload.				
			This vulnerability				
			is due to lack of				
			proper error				
			checking when				
			processing an				
			ingress MPLS				
			frame. An attacker				
			could exploit this				
			vulnerability by				
			sending a crafted IPv6 packet that is				
			encapsulated				
			within an MPLS				
			frame to an MPLS-				
			enabled interface				
			of the targeted				
			device. A successful				
			exploit could allow				
			the attacker to				
			cause a denial of				
			service (DoS) condition.				
			condition.				
			Note: The IPv6				
			packet can be				
			generated multiple				
			hops away from				
			the targeted device and then				
			encapsulated				
			within MPLS. The				
			DoS condition may				
			occur when the NX-				
			OS device				
			processes the				
			packet.				
			CVE ID : CVE-				
			2024-20267				
Affected Version(s): 6.0\\(2\\)a6\\(1a\\)							
·							
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 Page 81 of 356	5-6 6-7 7-8	8 8-9 9-10		

Page 81 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/85
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

Page 82 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(2			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/86

0-1

1-2

2-3

3-4 4-5 Page **83** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(2	2a\\)	<u> </u>	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/87

0-1

1-2

2-3

3-4 4-5 Page **84** of **356** 5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(3	3\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/88

0-1

1-2

2-3

3-4 4-5 Page **86** of **356** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(3	3a\\)	-	-
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/89

0-1

1-2

2-3

3-4 4-5 Page **87** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	2\\)a6\\(4	4\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/90

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			condition.		
			Noto, The ID-c		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
					<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **89** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 6.0\\(2</mark>	\\)a6\\(4	ła\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/91

0-1

1-2

2-3

3-4 4-5 Page **90** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(5	5//)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/92
			This vulnerability is due to lack of proper error		

0-1

1-2

2-3

3-4 4-5 Page **91** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(5	ia\\)		
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/93

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **93** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(!	5b\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/94

0-1

1-2

2-3

3-4 4-5 Page **94** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(6	5\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/95

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.0\\(2	2\\)a6\\(7	7\\)	1	
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	O-CIS-NX-O- 070324/96

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
L	I		0	I	<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **97** of **356** 5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a6\\(8	3//)	l	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/97

0-1

1-2

2-3

3-4 4-5 Page **98** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a7\\(1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/98

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	C ID
			network tr	affic or					
			to reload.						
			This vulne	-					
			is due to la						
			proper err						
			checking w						
			processing						
			ingress MF						
			frame. An a						
			could explo						
			vulnerabili						
			sending a o						
			IPv6 packe						
			encapsulat						
			within an I frame to ai						
			enabled in						
			of the targed device. A s						
			exploit cou						
			the attacke						
			cause a dei						
			service (De						
			condition.						
			contaction						
			Note: The	IPv6					
			packet can	be					
			generated	multiple					
			hops away						
			the targete						
			and then						
			encapsulat	ed					
			within MP						
			DoS condit	ion may					
			occur whe	n the NX-					
			OS device						
			processes	the					
			packet.						
			CVE ID : C	VE-					
			2024-202						
Affected Ver	sion(s): 6.0\\(2	2\\)a7\\(1a\\)		1		1		
CVSS Scoring S	Scale 0-1	1-2 2	2 <mark>-3</mark> 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Page 100 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/99

3-4

Page 101 of 356

4-5

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a7\\(2			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/100

0-1

1-2

2-33-44-5Page 102 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 6.0\\(2</mark>	\\)a7\\(2	2a\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/101

0-1

1-2

2-3

3-4 4-5 Page **103** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(2	I\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/102

0-1

1-2

2-3

3-4 4-5 Page **105** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(1	10\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/103
			is due to lack of proper error checking when processing an		

0-1

1-2

2-33-44-5Page 106 of 356

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(1	LUa\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/104

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from the targeted device		
			and then		
			encapsulated within MPLS. The		
			DoS condition may		
			occur when the NX-		

0-1

1-2

2-3

3-4 4-5 Page **108** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	(\ \)a8\\(1	11\\)	L	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/105

0-1

1-2

2-3

3-4 4-5 Page **109** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	:\\)a8\\(1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/106

0-1

1-2

2-3 3-4 4-5 Page **110** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(1	1b\\)	L	·
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/107

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **112** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(2	2\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-O- 070324/108

0-1

1-2

2-3

3-4 4-5 Page **113** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(3	3\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/109

0-1

1-2

2-3

3-4 4-5 Page **114** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(4	ŧ//)		
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	O-CIS-NX-O- 070324/110

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing network traffic or		
			to reload.		
			to reload.		
			TTL:- 1 1.1.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		

0-1

1-2

2-3

3-4 4-5 Page **116** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(4	ła\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/111

0-1

1-2

2-3

3-4 4-5 Page **117** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(5	2024-20267		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/112

0-1

1-2

2-3

6-7 7-8

5-6

Weakness Publish Date CVSSv3 Descrip	tion & CVE ID	Patch		NCIIPC I	D
networ	k traffic or				
to reloa	ıd.				
	lnerability				
	o lack of				
proper					
	lg when				
process					
ingress					
	An attacker				
	xploit this				
	bility by				
	g a crafted				
	cket that is				
encaps					
	an MPLS				
	o an MPLS-				
	l interface				
of the ta					
	A successful				
	could allow				
the atta					
cause a	denial of				
service					
conditio	on.				
Note: 1	`he IPv6				
packet					
	ed multiple				
	vay from				
	geted device				
and the	-				
encapsi					
· · · · · · · · · · · · · · · · · · ·	MPLS. The				
	ndition may				
	when the NX-				
OS devi					
process					
process packet.					
CVE ID	: CVE-				
2024-2					
Affected Version(s): 6.0\\(2\\)a8\\(6\\)					
CVSS Scoring Scale 0-1 1-2 2-3 3-	4 4-5	5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/113
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 120 of 356	5-6 6-7 7-8	8-9 9-10

Page 120 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(7			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/114

0-1

1-2

2-33-44-5Page 121 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 6.0\\(2</mark>	\\)a8\\(7	/a\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/115

0-1

1-2

2-3

3-4 4-5 Page **122** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(7	⁷ b\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/116

0-1

1-2

2-3

3-4 4-5 Page **124** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)a8\\(8	3//)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/117

0-1

1-2

2-3 3-4 4-5 Page **125** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	<mark>sion(s): 6.0\\(2</mark>	\\Ja8\\(9			
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/118

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
	l			1	<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **127** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 6.0\\(2</mark>	(\ \)u2\\(1\\)	L	l
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/119

0-1

1-2

2-3

3-4 4-5 Page **128** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u2\\(2		1	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/120

0-1

1-2

2-33-44-5Page 129 of 356

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.0\\(2	\\)u2\\(3			
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/121

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **131** of **356** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	2\\)u2\\(4	4//)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/122

0-1

1-2

2-3

3-4 4-5 Page **132** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u2\\(!			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/123

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.0\\(2	\\)u2\\(6			
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	0-CIS-NX-0- 070324/124

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing network traffic or		
			to reload.		
			to reload.		
			TTL:- 1 1.1.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		

0-1

1-2

2-3

3-4 4-5 Page **135** of **356** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u3\\(2	1//)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/125

0-1

1-2

2-3

3-4 4-5 Page **136** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 6.0\\(2</mark>	\\)u3\\(2			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/126

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	CID
			network tr	affic or					
			to reload.						
			Thiomula	nability					
			This vulne is due to la	-					
			proper err						
			checking v						
			processing						
			ingress MF						
			frame. An						
			could expl	oit this					
			vulnerabil						
			sending a	crafted					
			IPv6 packe						
			encapsulat						
			within an l						
			frame to a						
			enabled in						
			of the targ						
			device. A s						
			exploit cou the attacke						
			cause a de						
			service (De						
			condition.	05)					
			condition						
			Note: The	IPv6					
			packet can	be					
			generated	multiple					
			hops away	r from					
			the targete	ed device					
			and then						
			encapsulat						
			within MP						
			DoS condit	-					
			occur whe	n the NX-					
			OS device	+l					
			processes	the					
			packet.						
			CVE ID : C						
			2024-202	67					
Affected Vers	sion(s): 6.0\\(2	2\\Ju3\\(3\\)						
CVSS Scoring S	icale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/127
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 139 of 356	5-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Page 139 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u3\\(4	4\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/128

0-1

1-2

2-33-44-5Page 140 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u3\\(!	5//)	•	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/129

0-1

1-2

2-3

3-4 4-5 Page **141** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE- 2024-20267				
Affected Version(s): 6.0\\(2\\)u3\\(6\\)							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/130		

0-1

1-2

2-3

3-4 4-5 Page **143** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	:\\)u3\\(7\\)	•	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/131

0-1

1-2

2-33-44-5Page 144 of 356

5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u3\\(8	3\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/132

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			condition.		
			Note: The IPv6		
			packet can be generated multiple		
			hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
L	<u> </u>		occur when the WA-		<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **146** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 6.0\\(2</mark>	\\)u3\\(9	9\\)	L	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/133

0-1

1-2

2-3

3-4 4-5 Page **147** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	:\\)u4\\(:			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/134

0-1

1-2

2-33-44-5Page 148 of 356

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u4\\(2	2\\)		·
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/135

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **150** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u4\\(3	3\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/136

0-1

1-2

2-3

3-4 4-5 Page **151** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u4\\(4	4\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/137

0-1

1-2

2-3

3-4 4-5 Page **152** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.0\\(2	2 \\)u5\\(2			
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	0-CIS-NX-0- 070324/138

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
L	I		0	I	<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **154** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u5\\(2	2\\)	1	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/139

0-1

1-2

2-3

3-4 4-5 Page **155** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u5\\(3			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/140

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description	n & CVE ID		Patch		NCIIP	CID
			network t	raffic or					
			to reload.						
			This vuln	-					
			is due to la						
			proper er						
			checking v						
			processing						
			ingress M						
			frame. An						
			could expl						
			vulnerabil						
			sending a						
			IPv6 pack						
			encapsula						
			within an						
			frame to a						
			enabled in						
			of the targ						
			device. A s						
			exploit co						
			the attack						
			cause a de						
			service (D	-					
			condition.						
			Note: The	IPv6					
			packet car						
			generated						
			hops away						
			the target						
			and then						
			encapsula	ted					
			within MP						
			DoS condi						
			occur whe	-					
			OS device						
			processes	the					
			processes packet.						
			CVE ID : C	VE-					
			2024-202						
Affected Ver	sion(s): 6.0\\(2	2 <mark>\\)u5\\(</mark>	4\\)						
CVSS Scoring S	Scale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
CARR PCOLINE 2		1-2	2 3 3-4	4-5	5-0	0-7	7-0	6-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/141
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 158 of 356	5-6 6-7 7-8	8 8-9 9-10

Page 158 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	<mark>\\)u6\\(</mark> 1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/142

0-1

1-2

2-33-44-5Page 159 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(2	10\\)	I	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/143

0-1

1-2

2-3

3-4 4-5 Page **160** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(1a\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/144

0-1

1-2

2-3

3-4 4-5 Page **162** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(2	2\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/145

0-1

1-2

2-33-44-5Page 163 of 356

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(2	2a\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/146

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from the targeted device		
			and then		
			encapsulated within MPLS. The		
			DoS condition may		
			occur when the NX-		

0-1

1-2

2-33-44-5Page 165 of 356

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(3	3\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/147

0-1

1-2

2-3

3-4 4-5 Page **166** of **356** 6-7 7-8

5-6

Affected Version Buffer Copy without			the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX-		
Buffer Copy			packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX-		
Buffer Copy			OS device processes the packet. CVE ID : CVE- 2024-20267		
Сору	on(s): 6.0\\(2	\\)u6\\(3	3a\\)		
Checking	9-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/148

0-1

1-2

2-33-44-5Page 167 of 356

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.0\\(2	\\)u6\\(4			
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/149

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **169** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(4	4a\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/150

0-1

1-2

2-3

3-4 4-5 Page **170** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(!		Γ	Γ
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/151

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.0\\(2	://)u6//(!			
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	0-CIS-NX-0- 070324/152

CVSS Scoring Scale	
--------------------	--

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
L	I		0	I	<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **173** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	<mark>\\)u6\\(</mark> !	5b\\)	1	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/153

0-1

1-2

2-3

3-4 4-5 Page **174** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(!	5c\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/154

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	C ID
			network tr	affic or					
			to reload.						
			This vulne	-					
			is due to la						
			proper err						
			checking w						
			processing						
			ingress MF						
			frame. An a						
			could expl						
			vulnerabili						
			sending a d						
			IPv6 packe						
			encapsulat						
			within an I						
			frame to a						
			enabled in						
			of the targ						
			device. A s						
			exploit cou						
			the attacke						
			cause a dei						
			service (Do	55)					
			condition.						
			Note: The	IPv6					
			packet can						
			generated						
			hops away						
			the targete						
			and then						
			encapsulat	ed					
			within MP						
			DoS condit						
			occur whe	-					
			OS device						
			processes	the					
			packet.						
			CVE ID : C	VE-					
			2024-202						
Affected Ver	sion(s): 6.0\\(2	2\\)u6\\(6\\)		•		•		
		12				C 7	7.0	0.0	0.40
CVSS Scoring S	Scale 0-1	1-2 2	2 <mark>-3</mark> 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Page **176** of **356**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/155
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 177 of 356	5-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Page 177 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(7			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/156

0-1

1-2

2-33-44-5Page 178 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Version(s): 6.0\\(2\\)u6\\(8\\)					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/157

0-1

1-2

2-3

3-4 4-5 Page **179** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.0\\(2	\\)u6\\(9	9\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/158

0-1

1-2

2-3

3-4 4-5 Page **181** of **356** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(1	0\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/159
			is due to lack of proper error checking when processing an		

0-1

1-2

2-33-44-5Page 182 of 356

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(1	2\\)	2021 20207		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/160

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from the targeted device		
			and then		
			encapsulated within MPLS. The		
			DoS condition may		
			occur when the NX-		

0-1

1-2

2-33-44-5Page 184 of 356

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(1	4\\)	<u> </u>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/161

0-1

1-2

2-3

3-4 4-5 Page **185** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(1	6\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/162

0-1

1-2

2-33-44-5Page 186 of 356

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.2\\(1	8//)			
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/163

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **188** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(2	://)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/164

0-1

1-2

2-3

3-4 4-5 Page **189** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 6.2\\(2	0\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/165

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 6.2\\(2	0a\\)		1	
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	0-CIS-NX-0- 070324/166

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
L	I		0	I	<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **192** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(2	2\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/167

0-1

1-2

2-3

3-4 4-5 Page **193** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(2	4\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-O- 070324/168

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE	ID	Patch		NCIIP	CID
			network traffic or					
			to reload.					
			This vulnerabilit	у				
			is due to lack of					
			proper error					
			checking when					
			processing an					
			ingress MPLS					
			frame. An attacke					
			could exploit this					
			vulnerability by					
			sending a crafted					
			IPv6 packet that i	S				
			encapsulated					
			within an MPLS					
			frame to an MPLS					
			enabled interface					
			of the targeted					
			device. A success					
			exploit could allo	w				
			the attacker to					
			cause a denial of					
			service (DoS)					
			condition.					
			Note: The IPv6					
			packet can be					
			generated multip	le				
			hops away from					
			the targeted devi	ce				
			and then					
			encapsulated					
			within MPLS. The					
			DoS condition ma	-				
			occur when the N	X-				
			OS device					
			processes the					
			packet.					
			CVE ID : CVE-					
			2024-20267					
Affected Ver	sion(s): 6.2\\(2	4a\\)						
CVSS Scoring S	Scale 0-1	1-2 2	2- 3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Page 195 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/169
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 196 of 356	5-6 6-7 7-8	8-9 9-10

Page 196 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(2	a\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/170

0-1

1-2

2-33-44-5Page 197 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 6.2\\(6</mark>	\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/171

0-1

1-2

2-3

3-4 4-5 Page **198** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(6	a\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/172

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(6	b\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/173

0-1

1-2

2-33-44-5Page 201 of 356

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
Affected Ver	$rian(a)$, $(2) \setminus (0)$		2024-20267		
Allected ver	sion(s): 6.2\\(8	NU			
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/174

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from the targeted device		
			and then		
			encapsulated within MPLS. The		
			DoS condition may		
			occur when the NX-		

0-1

1-2

2-3

3-4 4-5 Page **203** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(8	a\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/175

0-1

1-2

2-3

3-4 4-5 Page **204** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 6.2\\(8	b\\)		I	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/176

0-1

1-2

2-33-44-5Page 205 of 356

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 7.0\\(3	\\)f1\\(1			
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/177

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **207** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped,	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/178

0-1

1-2

2-3

3-4 4-5 Page **208** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a DoS condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f2\\(1	\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/179

0-1

1-2

2-3

3-4 4-5 Page **209** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/180
			exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could		

0-1

1-2

2-3

3-4 4-5 Page **210** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f2\\(2			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/181

0-1

1-2

2-33-44-5Page 211 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated,	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/182

0-1

1-2

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network.		
			CVE ID : CVE- 2024-20321		
	sion(s): 7.0\\(3	\\)f3\\(1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/183

0-1

1-2

2-3 3-4 4-5 Page **213** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			771 1 1 1 1 1		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
L	1			I	

0-1

1-2

2-3 3-4 4-5 Page 214 of 356 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/184

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. CVE ID : CVE-		
			2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f3\\(2			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/185

0-1

1-2

2-3

3-4 4-5 Page **216** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/186

0-1

1-2

2-3

3-4 4-5 Page **217** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f3\\(3	\mathbb{N}		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/187

0-1

1-2

2-33-44-5Page 218 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/188

0-1

1-2

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f3\\(3	a\\)	<u> </u>	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/189

0-1

1-2

2-3

3-4 4-5 Page **220** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-3 3-4 4-5 Page **221** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/190

0-1

1-2

2-3

3-44-5Page 222 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f3\\(3	c\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/191

0-1

1-2

2-3

3-44-5Page 223 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/192

0-1

1-2

2-3

3-4 4-5 Page **224** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f3\\(4	$\langle 0 \rangle$		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/193

0-1

1-2

2-3 3-4 4-5 Page **225** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/194

0-1

1-2

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)f3\\(5	\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/195

0-1

1-2

2-3

3-4 4-5 Page **227** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-33-44-5Page 228 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/196

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 7.0\\(3	\\)i2\\(1	\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/197

0-1

1-2

2-3

3-4 4-5 Page **230** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 7.0\\(3</mark>	\\)i2\\(1		Γ	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/198

0-1

1-2

2-33-44-5Page 231 of 356

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
			OS device		
			processes the		
			packet.		
			CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i2\\(2			
Buffer			A vulnerability	1	
Сору	29-Feb-2024	024 8.6	with the handling	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco	O-CIS-NX-O-
without			of MPLS traffic for		
Checking			Cisco NX-OS		070324/199
Size of			Software could		070327/177
Input			allow an	SecurityAdvisor y/cisco-sa-ipv6-	
('Classic			unauthenticated,	y/cisco-sa-ipv0-	

0-1

1-2

2-33-44-5Page232 of356

5-6

6-7

Buffer remote attacker to mpls-dos- Overflow') cause the netstack R9ycXkwM process to unovnoctodly	
process to	
unovnoctodly	
unexpectedly	
restart, which	
could cause the	
device to stop	
processing	
network traffic or	
to reload.	
This vulnerability	
is due to lack of	
proper error	
checking when	
processing an	
ingress MPLS	
frame. An attacker	
could exploit this	
vulnerability by	
sending a crafted	
IPv6 packet that is	
encapsulated within an MPLS	
frame to an MPLS-	
enabled interface	
of the targeted	
device. A successful	
exploit could allow	
the attacker to	
cause a denial of	
service (DoS)	
condition.	
Note: The IPv6	
packet can be	
generated multiple	
hops away from	
the targeted device	
and then	
encapsulated	
within MPLS. The	
DoS condition may	

0-1

1-2

2-3

3-4 4-5 Page **233** of **356** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occur when the NX- OS device processes the packet. CVE ID : CVE-		
Affected Ver	sion(s): 7.0\\(3	\\);2\\(?	2024-20267		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/200

0-1

1-2

2-33-44-5Page234 of356

6-7 7-8

5-6

Buffer Copy without Checking Size of Input (Classic Buffer Overflow')29-Feb-20248.6A vulnerability with the superceduly restance of the restance or classe to stop processing network traffic or to reload.https://sec.clou daps.cisco.com /security/center /content/Clsco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkvMO-CIS-NX-0- 070324/201	Weakness F	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Nerflow')29-Feb-20248.6A vulnerability with state the netstack processing network traffic orhttps://sec.clou daps.cisco.com /security/dvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwMO-CIS-NX-O- 070324/201				the attacker to cause a denial of service (DoS)		
Buffer Copy without Checking Size of Input ('Classic 				packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')29-Feb-20248.6with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which orestart, which processing network traffic orhttps://sec.clou dapps.cisco.com r/content/Cisco 0-CIS-NX-0- 070324/201Buffer Overflow')29-Feb-20248.68.6of MPLS traffic for cause the netstack process to unexpectedly restart, which processing network traffic orof MPLS traffic for cause the netstack processing network traffic orof MPLS traffic for cause the netstack processing network traffic or	Affected Versio	on(s): 7.0\\(3)	\\)i2\\(2			Γ
	Copy without Checking Size of 24 Input ('Classic Buffer	9-Feb-2024	8.6	with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or	dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos-	

Page 235 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i2\\(2	c\\)		
Buffer Copy without Checking Size of	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor	O-CIS-NX-O- 070324/202

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated		

0-1

1-2

2-3

3-4 4-5 Page **237** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i2\\(2	d\\)	_	-
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/203

0-1

1-2

2-3

3-4 4-5 Page **238** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i2\\(2			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/204

0-1

1-2

2-3

3-4 4-5 Page **239** of **356** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i2\\(3	\\)	1	
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	O-CIS-NX-O- 070324/205

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
			-		J

0-1

1-2

2-3

3-4 4-5 Page **241** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	$\frac{1}{100}$ sion(s): 7.0\\(3	\\)i2\\(4	\\)	1	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-O- 070324/206

0-1

1-2

2-3

3-4 4-5 Page **242** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i2\\(5			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/207

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch		NCIIPC ID	
			network traffic or				
			to reload.				
			This vulnerability				
			is due to lack of				
			proper error				
			checking when				
			processing an				
			ingress MPLS				
			frame. An attacker				
			could exploit this				
			vulnerability by				
			sending a crafted				
			IPv6 packet that is				
			encapsulated				
			within an MPLS				
			frame to an MPLS-				
			enabled interface				
			of the targeted				
			device. A successful				
			exploit could allow				
			the attacker to				
			cause a denial of				
			service (DoS)				
			condition.				
			Note: The ID:				
			Note: The IPv6				
			packet can be				
			generated multiple				
			hops away from				
			the targeted device				
			and then				
			encapsulated within MPLS. The				
			DoS condition may				
			occur when the NX-				
			OS device				
			processes the				
			packet.				
			CVE ID : CVE-				
A.CC			2024-20267				
Affected Ver	$sion(s): 7.0 \setminus (3)$	\\)I3\\(1	\U				
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7	7-8	8-9 9-1	10
		2		30 07	, 0	55	_

Page 244 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-O- 070324/208
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 245 of 356	5-6 6-7 7-8	8-9 9-10

Page 245 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(1	\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/209

0-1

1-2

2-33-44-5Page246 of356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(2	\\)	I	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/210

0-1

1-2

2-3

3-4 4-5 Page **247** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of		
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		
			os device processes the packet.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(3			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/211

0-1

1-2

2-3

3-4 4-5 Page **249** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(4		·	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/212

0-1

1-2

2-33-44-5Page 250 of 356

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(5	\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/213

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			condition.		
			Note: The IPv6		
			packet can be generated multiple		
			hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
L	<u> </u>		occur when the WA-		<u> </u>

0-1

1-2

2-33-44-5Page 252 of 356

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(6	\\)	L	l
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/214

0-1

1-2

2-3

3-4 4-5 Page **253** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(7			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/215

0-1

1-2

2-3 3-4 4-5 Page 254 of 356 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(8	\\)		
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/216

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **256** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(8	a\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/217

0-1

1-2

2-3

3-4 4-5 Page **257** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE-		
Affected Ver	sion(s): 7.0\\(3	\\)i4\\(8	2024-20267		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/218

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 7.0\\(3	\\)i4\\(8	z\\)		
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	O-CIS-NX-O- 070324/219

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
			-		J

0-1

1-2

2-3

3-4 4-5 Page **260** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	$\frac{1}{100}$ sion(s): 7.0\\(3	\\)i4\\(9	\\)	1	<u>.</u>
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/220

0-1

1-2

2-3

3-4 4-5 Page **261** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 7.0\\(3</mark>	\\)i5\\(1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/221

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID		Patch		NCIIP	CID
			network traffic or					
			to reload.					
			This see he see hiliter					
			This vulnerability is due to lack of					
			proper error					
			checking when					
			processing an					
			ingress MPLS					
			frame. An attacker					
			could exploit this					
			vulnerability by					
			sending a crafted					
			IPv6 packet that is					
			encapsulated					
			within an MPLS					
			frame to an MPLS-					
			enabled interface					
			of the targeted					
			device. A successful					
			exploit could allow					
			the attacker to					
			cause a denial of					
			service (DoS)					
			condition.					
			Note: The IPv6					
			packet can be					
			generated multiple					
			hops away from					
			the targeted device					
			and then					
			encapsulated					
			within MPLS. The					
			DoS condition may					
			occur when the NX-					
			OS device					
			processes the					
			packet.					
			CVE ID : CVE-					
			2024-20267					
Affected Ver	sion(s): 7.0\\(3	3 <mark>\\)</mark> i5\\(2	\\)	·		I		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Page 263 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/222
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 264 of 356	5-6 6-7 7-8	8-9 9-10

Page 264 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i6\\(1	\\)	L	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/223

0-1

1-2

2-33-44-5Page 265 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i6\\(2	\\)	I	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/224

0-1

1-2

2-3

3-4 4-5 Page **266** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of		
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		
			os device processes the packet.		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i7\\(1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/225

0-1

1-2

2-3

3-4 4-5 Page **268** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 7.0\\(3</mark>	\\)i7\\(1	0\\)		·
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/226

0-1

1-2

2-33-44-5Page 269 of 356

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i7\\(2	\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/227

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			condition.		
			Note: The ID(
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
L	<u> </u>		seem when the fix		<u> </u>

0-1

1-2

2-3

3-4 4-5 Page **271** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i7\\(3	\\)	L	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/228

0-1

1-2

2-3

3-4 4-5 Page **272** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i7\\(4			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/229

0-1

1-2

2-33-44-5Page 273 of 356

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 7.0\\(3	\\)i7\\(5			
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/230

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **275** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i7\\(5	a\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/231

0-1

1-2

2-3

3-4 4-5 Page **276** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE-		
Affected Mer	$rice(a) = 7 = 0 \setminus (a)$	$\left(\right)$	2024-20267		
Affected ver	<mark>sion(s): 7.0\\(3</mark>	\\)!/\\(6			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/232

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 7.0\\(3</mark>	\\)i7\\(7	\\)	I	
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	O-CIS-NX-O- 070324/233

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		
			-		J

0-1

1-2

2-3

3-4 4-5 Page **279** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	 <mark>sion(s): 7.0\\(3</mark>	\\)i7\\(8			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/234

0-1

1-2

2-3

3-4 4-5 Page **280** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.0\\(3	\\)i7\\(9			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/235

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	CID
			network tr	affic or					
			to reload.						
			This vulne	-					
			is due to la						
			proper err						
			checking w						
			processing						
			ingress MF						
			frame. An a						
			could expl						
			vulnerabili						
			sending a d						
			IPv6 packe						
			encapsulat						
			within an I						
			frame to a						
			enabled in						
			of the targ						
			device. A s						
			exploit cou						
			the attacke						
			cause a dei						
			service (Do	55)					
			condition.						
			Note: The	IPv6					
			packet can						
			generated						
			hops away						
			the targete						
			and then						
			encapsulat	ed					
			within MP						
			DoS condit						
			occur whe	-					
			OS device	-					
			processes	the					
			packet.						
			CVE ID : C	VE-					
			2024-202						
Affected Ver	$sion(s): 7.1 \setminus (0)$)\\)n1\\(1\\)						
0.455.5									
CVSS Scoring S	Scale 0-1	1-2 2	2 <mark>-3</mark> 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Page 282 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/236
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 283 of 356	5-6 6-7 7-8	3 8-9 <mark>9-10</mark>

Page 283 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.1\\(0	\\)n1\\(1a\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/237

0-1

1-2

2-33-44-5Page 284 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.1\\(0	\\)n1\\(1b\\)		•
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/238

0-1

1-2

2-3

3-4 4-5 Page **285** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of		
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		
			os device processes the packet.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.1\\(1	\\)n1\\(1\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/239

0-1

1-2

2-3

3-4 4-5 Page **287** of **356** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.1\\(2	\\)n1\\(2	i\\)	•	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/240

0-1

1-2

2-33-44-5Page 288 of 356

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
			2024-20267		
Affected Ver	sion(s): 7.1\\(3	\\)n1\\(:	1\\)		
Buffer Copy without Checking Size of Input ('Classic	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/241

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer			cause the netstack		
Overflow')			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing		
			network traffic or		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an		
			ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			condition.		
			Note: The IPv6		
			packet can be generated multiple		
			hops away from		
			the targeted device		
			and then		
			encapsulated		
			within MPLS. The		
			DoS condition may		
			occur when the NX-		
L	<u> </u>		occur when the WA-		<u> </u>

0-1

1-2

2-33-44-5Page 290 of 356

6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	<mark>sion(s): 7.1\\(3</mark>	\\)n1\\(2	2\\)	L	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/242

0-1

1-2

2-3

3-4 4-5 Page **291** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.1\\(4	\\)n1\\(:			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/243

0-1

1-2

2-33-44-5Page 292 of 356

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.1\\(5	\\)n1\\(2	1\\)		
Buffer Copy without Checking Size of Input	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6-	O-CIS-NX-O- 070324/244

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	mpls-dos- R9ycXkwM	
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The		

0-1

1-2

2-3

3-4 4-5 Page **294** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.1\\(5	\\)n1\\(1b\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/245

0-1

1-2

2-3

3-4 4-5 Page **295** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.2\\(0	\\)d1\\(1	L\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/246

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
	sion(s): 7.2\\(1	\\)d1\\(2			
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.clou dapps.cisco.com /security/cente	0-CIS-NX-0- 070324/247

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking			Cisco NX-OS	r/content/Cisco	
Size of			Software could	SecurityAdvisor	
Input			allow an	y/cisco-sa-ipv6-	
('Classic			unauthenticated,	mpls-dos-	
Buffer			remote attacker to	R9ycXkwM	
Overflow')			cause the netstack		
			process to		
			unexpectedly		
			restart, which		
			could cause the		
			device to stop		
			processing network traffic or		
			to reload.		
			to reload.		
			This vulnerability		
			is due to lack of		
			proper error		
			checking when		
			processing an ingress MPLS		
			frame. An attacker		
			could exploit this		
			vulnerability by		
			sending a crafted		
			IPv6 packet that is		
			encapsulated		
			within an MPLS		
			frame to an MPLS-		
			enabled interface		
			of the targeted		
			device. A successful		
			exploit could allow		
			the attacker to		
			cause a denial of		
			service (DoS)		
			condition.		
			Note: The IPv6		
			packet can be		
			generated multiple		
			hops away from		
			the targeted device		

0-1

1-2

2-3

3-4 4-5 Page **298** of **356** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.2\\(2	\\)d1\\(1\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-O- 070324/248

0-1

1-2

2-3

3-4 4-5 Page **299** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE-		
Affected Ver	sion(s): 7.2\\(2	\\)d1\\(2	2024-20267 2\\)		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/249

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Descriptio	n & CVE ID		Patch		NCIIP	C ID
			network t	raffic or					
			to reload.						
			This vuln	-					
			is due to l						
			proper er						
			checking						
			processin						
			ingress M						
			frame. An						
			could exp						
			vulnerabi						
			sending a						
			IPv6 pack						
			encapsula						
			within an						
			frame to a						
			enabled ir						
			of the targ						
			device. A s						
			exploit co						
			the attack						
			cause a de						
			service (D	-					
			condition						
			N . TI						
			Note: The						
			packet car						
			generated						
			hops away						
			the target	ed device					
			and then	(
			encapsula						
			within MF						
			DoS condi	-					
			occur whe	en the NX	-				
			OS device	.1					
			processes	the					
			packet.						
			CVE ID : C	VE-					
			2024-202	267					
Affected Ver	sion(s): 7.3\\(0	\\)d1\\(1\\)						
0.000						-			
CVSS Scoring S	icale 0-1	1-2 2	2 <mark>-3</mark> 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Page **301** of **356**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/250
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 Page 302 of 356	5-6 6-7 7-8	8-9 9-10

Page 302 of 356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.3\\(0	\\)dx\\(1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/251

0-1

1-2

2-33-44-5Page 303 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 7.3\\(0	\\)n1\\(í	1//)		1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/252

0-1

1-2

2-3

3-4 4-5 Page **304** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of		
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		
			os device processes the packet.		

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE- 2024-20267		
Affected Ver	sion(s): 9.2\\(1	\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/253

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/254

0-1

1-2

2-33-44-5Page 307 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.2\\(2	\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-O- 070324/255

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/256

0-1

1-2

2-33-44-5Page 309 of 356

5-6

7-8

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.2\\(2	t\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/257

0-1

1-2

2-3

3-4 4-5 Page **310** of **356** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/258

0-1

1-2

2-33-44-5Page 312 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. CVE ID : CVE-		
			2024-20321		
Affected Ver	sion(s): 9.2\\(2	v\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/259

0-1

1-2

2-3

3-4 4-5 Page **313** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/260

0-1

1-2

2-3

3-4 4-5 Page **314** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.2\\(3	\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/261

0-1

1-2

2-33-44-5Page 315 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/262

0-1

1-2

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.2\\(4	·\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/263

0-1

1-2

2-3

3-4 4-5 Page **317** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-33-44-5Page 318 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/264

0-1

1-2

2-33-44-5Page 319 of 356

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(1	\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/265

0-1

1-2

2-3

3-4 4-5 Page **320** of **356** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/266

0-1

1-2

2-33-44-5Page 321 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(1	0\\)		<u> </u>	<u> </u>
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/267

0-1

1-2

2-33-44-5Page 322 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/268

0-1

1-2

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(1	1\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/269

0-1

1-2

2-3

3-4 4-5 Page **324** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-33-44-5Page 325 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/270

0-1

1-2

2-3

3-4 4-5 Page **326** of **356** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(1	2\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/271

0-1

1-2

2-3

3-4 4-5 Page **327** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/272

0-1

1-2

2-3

3-4 4-5 Page **328** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(2	\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/273

0-1

1-2

2-3 3-4 4-5 Page **329** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/274

0-1

1-2

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(3	//)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/275

0-1

1-2

2-3

3-4 4-5 Page **331** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-33-44-5Page 332 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/276

0-1

1-2

2-33-44-5Page 333 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(4	(//			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/277

0-1

1-2

2-3

3-4 4-5 Page **334** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/278

0-1

1-2

2-3

3-4 4-5 Page **335** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(5	\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/279

0-1

1-2

2-33-44-5Page336 of356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/280

0-1

1-2

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(6	//)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/281

0-1

1-2

2-3

3-4 4-5 Page **338** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-33-44-5Page 339 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/282

0-1

1-2

2-33-44-5Page 340 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network.		
			CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(7	`\\)			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/283

0-1

1-2

2-3

3-4 4-5 Page **341** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition.		
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet.		
			CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/284

0-1

1-2

2-3

3-4 4-5 Page **342** of **356** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(7	a\\)	<u> </u>	<u> </u>	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	0-CIS-NX-0- 070324/285

0-1

1-2

2-33-44-5Page 343 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/286

0-1

1-2

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition on an affected device.		
			This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE- 2024-20321		
Affected Ver	sion(s): 9.3\\(8	(/)		I	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/287

0-1

1-2

2-3

3-4 4-5 Page **345** of **356** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly restart, which could cause the device to stop processing network traffic or to reload.		
			This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS)		
			condition. Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device		

0-1

1-2

2-33-44-5Page 346 of 356

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	O-CIS-NX-O- 070324/288

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE- 2024-20321					
Affected Version(s): 9.3\\(9\\)								
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS- enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa-ipv6- mpls-dos- R9ycXkwM	O-CIS-NX-O- 070324/289			

0-1

1-2

2-33-44-5Page 348 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX- OS device processes the packet. CVE ID : CVE- 2024-20267		
Allocation of Resources Without Limits or Throttling	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- nxos-ebgp-dos- L3QCwVJ	0-CIS-NX-0- 070324/290

0-1

1-2

2-33-44-5Page 349 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. CVE ID : CVE-		
			2024-20321		
Vendor: De					
Product: de	bian_linux sion(s): 10.0				
Allected vel	51011(5). 10.0		The		
Improper Authentica tion	22-Feb-2024	6.5	implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This	https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 e55255a81270 b768439c	O-DEB-DEBI- 070324/291

0-1

1-2

2-33-44-5Page 350 of 356

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an adversary to impersonate Enterprise Wi-Fi networks. CVE ID : CVE-		
			2023-52160		
Vendor: Fed					
Product: fee	dora				
Affected Ver	sion(s): 39				
Improper Authentica tion	22-Feb-2024	6.5	The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks.	https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 e55255a81270 b768439c	O-FED-FEDO- 070324/292

0-1

1-2

2-33-44-5Page 351 of 356

6-7 7-8

5-6

Authentica22-Feb-20246.5eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows ana1bcb0baffdea9 e55255a81270 b768439c070324/293070324/293070324/293	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Improper Authentica tion 22-Feb-2024 6.5 The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 0-G00-ANDR										
Affected Version(s): *Improper Authentica22-Feb-20246.5The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an0-GOO-ANDR 070324/293	Vendor: Google									
Improper Authentica tion22-Feb-20246.5The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a 	Product: android									
Improper Authentica22-Feb-20246.5implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows anhttps://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bc0baffdea9O-GOO-ANDR 070324/293	Affected Ver	sion(s): *								
impersonate Enterprise Wi-Fi networks. CVE ID : CVE- 2023-52160	Authentica tion		6.5	<pre>implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks. CVE ID : CVE-</pre>	it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 e55255a81270	0-G00-ANDR- 070324/293				
Product: chrome_os	Product: ch	rome_os								
Affected Version(s): *	Affected Ver	sion(s): *								

0-1

1-2

2-3

3-4 4-5 Page **352** of **356** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID Patch		NCIIPC ID		
Improper Authentica tion	22-Feb-2024	6.5	The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks. CVE ID : CVE- 2023-52160	https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 e55255a81270 b768439c	0-G00-CHR0- 070324/294		
Vendor: Linux							
Product: linux_kernel Affected Version(s): *							
Allected ver			The				
Improper Authentica tion	22-Feb-2024	6.5	implementation of PEAP in wpa_supplicant through 2.10	https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9	O-LIN-LINU- 070324/295		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 353 of 356										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks. CVE ID : CVE- 2023-52160	e55255a81270 b768439c	
Vendor: Ree	dhat			I	
Product: en	terprise_linux				
Affected Ver	sion(s): 8.0				
Improper Authentica tion	22-Feb-2024	6.5	The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant	https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 e55255a81270 b768439c	O-RED-ENTE- 070324/296

0-1

1-2

2-3 3-4 4-5 Page **354** of **356** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP- TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks. CVE ID : CVE- 2023-52160		
Affected Ver	sion(s): 9.0				
Improper Authentica tion	22-Feb-2024	6.5	The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt	https://w1.fi/cg it/hostap/com mit/?id=8e6485 a1bcb0baffdea9 e55255a81270 b768439c	O-RED-ENTE- 070324/297

0-1

1-2

2-33-44-5Page 355 of 356

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can		
			then be abused to		
			skip Phase 2		
			authentication. The		
			attack vector is		
			sending an EAP-		
			TLV Success packet		
			instead of starting		
			Phase 2. This		
			allows an		
			adversary to		
			impersonate		
			Enterprise Wi-Fi		
			networks.		
			CVE ID : CVE-		
			2023-52160		

0-1

1-2

2-3

5-6

6-7 7-8 8-9