https://nciipc.gov.in/

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 – 29 Feb 2024 Vol. 11 No. 04

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Apache					
Product: commons_compress					
Affected Version(s): From (including) 1.21.0 Up to (excluding) 1.26.0					
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.apache.org/thread/ch5yo2d21p7vlqrhll9b17otbyq4npfg	A-APA-COMM-070324/1
Affected Version(s): From (including) 1.3 Up to (excluding) 1.26.0					
Loop with Unreachable 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.apache.org/thread/cz8qkcwphy4cx8gltn932ln51cbtq6kf	A-APA-COMM-070324/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-25710		
Vendor: connectwise					
Product: screenconnect					
Affected Version(s): * Up to (excluding) 23.9.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Feb-2024	8.4	ConnectWise 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. **CVE ID : CVE-2024-1708**	https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8	A-CON-SCRE-070324/3
N/A	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.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8	A-CON-SCRE-070324/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (including) 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 Version(s): 16.9.0					
Improper Neutralization 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 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
			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_member 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

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

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			environment details of projects **CVE ID : CVE-2023-4895**		
Affected Version(s): From (including) 12.0 Up to (including) 16.76					
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-070324/13
Affected Version(s): From (including) 15.1.0 Up to (excluding) 16.7.6					
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.	N/A	A-GIT-GITL-070324/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0410		
Affected Version(s): From (including) 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 Version(s): From (including) 16.4.0 Up to (excluding) 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

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 Version(s): From (including) 16.5.0 Up to (excluding) 16.7.6					
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_member 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 Version(s): From (including) 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

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
			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
Affected Version(s): From (including) 16.8.0 Up to (excluding) 16.8.3					

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-2024-0410**	N/A	A-GIT-GITL-070324/20
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 Version(s): From (including) 16.8.0 Up to (including) 16.8.3					
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

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_member 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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Intel					
Product: inet_wireless_daemon					
Affected Version(s): * Up to (excluding) 2.14					
Improper Authentication	22-Feb-2024	7.5	The Access Point functionality in eapol_auth_key_handle 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.kernel.org/pub/scm/network/wireless/iwd.git/commit/?id=6415420f1c92012f64063c131480ffcef58e60ca	A-INT-INET-070324/24
Vendor: Oracle					
Product: mysql_server					
Affected Version(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.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/25

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/AC: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	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/26

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/AC: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.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/27

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/AC: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	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/28

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/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20978**		
Affected Version(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. 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.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/29

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/AC: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.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC: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.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/31

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/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20978**	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/32

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. 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/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20972**	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/33
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com/security-	A-ORA-MYSQ-070324/34

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/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20974**	alerts/cpujan2024.html	
N/A	17-Feb-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/35

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/AC: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.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-070324/36

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/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20978**		
Vendor: W1.fi					
Product: wpa_supplicant					
Affected Version(s): * Up to (excluding) 2.10					
Improper Authentication	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/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9e55255a81270b768439c	A-W1.-WPA_-070324/37

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**		
Operating System					
Vendor: Cisco					
Product: nx-os					
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/38

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 packet. **CVE ID : CVE-2024-20267**		
Allocation of Resources Without	29-Feb-2024	8.6	A vulnerability in the External Border Gateway Protocol (eBGP)	https://sec.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-070324/39

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. 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**	SecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	
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.cloudapps.cisco.com/security/center/content/Cisco	O-CIS-NX-O-070324/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device and then	SecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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
			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 through an affected device. A successful exploit could allow the attacker to cause eBGP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/41

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/42

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 eBGP traffic is mapped to a shared hardware	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/43

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 Version(s): 10.2\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/44

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-NX-O-070324/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC 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. **CVE ID : CVE-2024-20321**	nxos-ebgp-dos-L3QCwVJ	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			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 generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may	mpls-dos-R9ycXkwM	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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, leading to a DoS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/48

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/49

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/50

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/51

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 Version(s): 10.2\\(3t\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/52

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
			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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/54

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/55

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 Version(s): 10.2\\(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 network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/56

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/57

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
			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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/58

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/60

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
			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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/61

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 Version(s): 10.3\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/62

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/63

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/64

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/66

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/67

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/68

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/69

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/70

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
			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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/71

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/73

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
			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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/74

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/75

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 Version(s): 6.0\\(2\\)a3\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/76

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 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)a3\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/77

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 Version(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. This vulnerability is due to lack of proper error	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/78

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 Version(s): 6.0\\(2\\)a4\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/79

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. 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	mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)a4\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/80

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 Version(s): 6.0\\(2\\)a4\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/81

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 Version(s): 6.0\\(2\\)a4\\(5\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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
			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\\)a4\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/83

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 Version(s): 6.0\\(2\\)a6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/84

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
			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. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)a6\\(1a\\)					

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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/85

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/86

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\\)a6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/87

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
			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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(s): 6.0\\(2\\)a6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/88

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 Version(s): 6.0\\(2\\)a6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/89

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 Version(s): 6.0\\(2\\)a6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/90

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 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)a6\\(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 device. A successful exploit could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/91

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
			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\\)a6\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/92

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 Version(s): 6.0\\(2\\)a6\\(5a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/93

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. 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	mpls-dos-R9ycXkwM	

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/94

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 Version(s): 6.0\\(2\\)a6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/95

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 Version(s): 6.0\\(2\\)a6\\(7\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/96

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
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)a6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/97

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/98

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 packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)a7\\(1a\\)					

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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/99

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/100

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\\)a7\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/101

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(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 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/102

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 Version(s): 6.0\\(2\\)a8\\(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. This vulnerability is due to lack of proper error checking when processing an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/103

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 Version(s): 6.0\\(2\\)a8\\(10a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)a8\\(11\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/105

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 Version(s): 6.0\\(2\\)a8\\(11a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/106

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 Version(s): 6.0\\(2\\)a8\\(11b\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/107

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. 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	mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)a8\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/108

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
			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\\)a8\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/109

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 Version(s): 6.0\\(2\\)a8\\(4\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)a8\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/111

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 Version(s): 6.0\\(2\\)a8\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/112

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 packet. **CVE ID : CVE-2024-20267**		
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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/113

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/114

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\\)a8\\(7a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/115

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(s): 6.0\\(2\\)a8\\(7b\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/116

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 Version(s): 6.0\\(2\\)a8\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/117

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 Version(s): 6.0\\(2\\)a8\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)u2\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/119

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 Version(s): 6.0\\(2\\)u2\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/120

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/121

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. 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	mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)u2\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/122

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
			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\\)u2\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/123

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 Version(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.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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
			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\\)u3\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/125

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 Version(s): 6.0\\(2\\)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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/126

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
			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. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)u3\\(3\\)					

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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/127

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 Version(s): 6.0\\(2\\)u3\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/128

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\\)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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/129

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.		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/130

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/131

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
			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 Version(s): 6.0\\(2\\)u3\\(8\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)u3\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/133

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 Version(s): 6.0\\(2\\)u4\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/134

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 Version(s): 6.0\\(2\\)u4\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/135

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. 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	mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)u4\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/136

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 Version(s): 6.0\\(2\\)u4\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/137

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 Version(s): 6.0\\(2\\)u5\\(1\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/138

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
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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
			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\\)u5\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/139

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
			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\\)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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/140

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 packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)u5\\(4\\)					

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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/141

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
			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\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/142

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
			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\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/143

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
			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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/144

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 Version(s): 6.0\\(2\\)u6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/145

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 Version(s): 6.0\\(2\\)u6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)u6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/147

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 Version(s): 6.0\\(2\\)u6\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/148

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/149

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. 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	mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)u6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/150

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 Version(s): 6.0\\(2\\)u6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/151

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 Version(s): 6.0\\(2\\)u6\\(5a\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/152

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
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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 Version(s): 6.0\\(2\\)u6\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/153

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
			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\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/154

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 packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.0\\(2\\)u6\\(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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/155

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
			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\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/156

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/157

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(s): 6.0\\(2\\)u6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/158

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 Version(s): 6.2\\(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. This vulnerability is due to lack of proper error checking when processing an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/159

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
			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 Version(s): 6.2\\(12\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.2\\(14\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/161

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 Version(s): 6.2\\(16\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/162

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 Version(s): 6.2\\(18\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/163

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. 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	mpls-dos-R9ycXkwM	

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/164

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 Version(s): 6.2\\(20\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/165

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 Version(s): 6.2\\(20a\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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
			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): 6.2\\(22\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/167

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
			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): 6.2\\(24\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/168

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
			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. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.2\\(24a\\)					

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/169

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 Version(s): 6.2\\(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 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/170

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): 6.2\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/171

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(s): 6.2\\(6a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/172

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 Version(s): 6.2\\(6b\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/173

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 Version(s): 6.2\\(8\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

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
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 6.2\\(8a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/175

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 Version(s): 6.2\\(8b\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/176

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/177

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. 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	mpls-dos-R9ycXkwM	

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
			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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a DoS condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/179

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 eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/180

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/181

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/182

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
			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**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/183

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
		🟧	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-OS device		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/185

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/186

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 Version(s): 7.0\\(3\\)f3\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/187

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/188

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
			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 Version(s): 7.0\\(3\\)f3\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/189

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(s): 7.0\\(3\\)f3\\(3c\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/191

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/192

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 Version(s): 7.0\\(3\\)f3\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/193

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/194

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/195

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/197

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
			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): 7.0\\(3\\)i2\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/198

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 Version(s): 7.0\\(3\\)i2\\(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,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may	mpls-dos-R9ycXkwM	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occur when the NX-OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 7.0\\(3\\)i2\\(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 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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): 7.0\\(3\\)i2\\(2b\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/201

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 Version(s): 7.0\\(3\\)i2\\(2c\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	O-CIS-NX-O-070324/202

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
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. 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	y/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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 Version(s): 7.0\\(3\\)i2\\(2d\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/203

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
			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): 7.0\\(3\\)i2\\(2e\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/204

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 Version(s): 7.0\\(3\\)i2\\(3\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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 Version(s): 7.0\\(3\\)i2\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/206

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/207

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
			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. **CVE ID : CVE-2024-20267**		

Affected Version(s): 7.0\\(3\\)i3\\(1\\)

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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/208

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
			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): 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/209

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): 7.0\\(3\\)i4\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/210

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/211

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/212

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 7.0\\(3\\)i4\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/214

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
			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): 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/215

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/216

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
('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. 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	mpls-dos-R9ycXkwM	

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 Version(s): 7.0\\(3\\)i4\\(8a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/217

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 Version(s): 7.0\\(3\\)i4\\(8b\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/218

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 Version(s): 7.0\\(3\\)i4\\(8z\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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 Version(s): 7.0\\(3\\)i4\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/220

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 Version(s): 7.0\\(3\\)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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/221

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 packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 7.0\\(3\\)i5\\(2\\)					

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/222

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 Version(s): 7.0\\(3\\)i6\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/223

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): 7.0\\(3\\)i6\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/224

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/225

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 Version(s): 7.0\\(3\\)i7\\(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. This vulnerability is due to lack of proper error checking when processing an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/226

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/227

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 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 7.0\\(3\\)i7\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/228

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/229

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
			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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/230

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. 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	mpls-dos-R9ycXkwM	

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 Version(s): 7.0\\(3\\)i7\\(5a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/231

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 Version(s): 7.0\\(3\\)i7\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/232

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 Version(s): 7.0\\(3\\)i7\\(7\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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
			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): 7.0\\(3\\)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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/234

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/235

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 packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 7.1\\(0\\)n1\\(1\\)					

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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/236

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/237

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): 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/238

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/239

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
			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): 7.1\\(2\\)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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/240

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
			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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer 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 and then encapsulated within MPLS. The DoS condition may occur when the NX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS device processes the packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 7.1\\(3\\)n1\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/242

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 Version(s): 7.1\\(4\\)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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/243

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 Version(s): 7.1\\(5\\)n1\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-	O-CIS-NX-O-070324/244

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. 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	mpls-dos-R9ycXkwM	

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/245

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 Version(s): 7.2\\(0\\)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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/246

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 Version(s): 7.2\\(1\\)d1\\(1\\)					
Buffer Copy without	29-Feb-2024	8.6	A vulnerability with the handling of MPLS traffic for	https://sec.cloudapps.cisco.com/security/cente	O-CIS-NX-O-070324/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')		🟧	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 generated multiple hops away from the targeted device	r/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/248

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 Version(s): 7.2\\(2\\)d1\\(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/249

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 packet. **CVE ID : CVE-2024-20267**		
Affected Version(s): 7.3\\(0\\)d1\\(1\\)					

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. Note: The IPv6 packet can be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/250

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/251

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
			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): 7.3\\(0\\)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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/252

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20267		
Affected Version(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-enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/253

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/254

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/255

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/256

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 Version(s): 9.2\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/257

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		

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
			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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(s): 9.2\\(2v\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/259

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/260

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/261

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/262

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/263

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/265

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/266

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 Version(s): 9.3\\(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. This vulnerability is due to lack of proper error checking when processing an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/267

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
			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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/268

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 Version(s): 9.3\\(11\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/269

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(s): 9.3\\(12\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/271

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/272

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/273

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
			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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/274

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/275

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
			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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/277

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/278

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/279

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/280

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 Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/281

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition in the network. **CVE ID : CVE-2024-20321**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/283

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/284

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 Version(s): 9.3\\(7a\\)					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/285

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/286

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
			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 Version(s): 9.3\\(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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/287

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		

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/288

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
			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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM	O-CIS-NX-O-070324/289

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ	O-CIS-NX-O-070324/290

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: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Improper Authentication	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	https://w1.fi/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9e55255a81270b768439c	O-DEB-DEBI-070324/291

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: Fedoraproject					
Product: fedora					
Affected Version(s): 39					
Improper Authentication	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/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9e55255a81270b768439c	O-FED-FEDO-070324/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52160		
Vendor: Google					
Product: android					
Affected Version(s): *					
Improper Authentication	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/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9e55255a81270b768439c	O-GOO-ANDR-070324/293
Product: chrome_os					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	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/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9e55255a81270b768439c	O-GOO-CHRO-070324/294
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): *					
Improper Authentication	22-Feb-2024	6.5	The implementation of PEAP in wpa_supplicant through 2.10	https://w1.fi/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9	O-LIN-LINU-070324/295

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**	e55255a81270b768439c	
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Improper Authentication	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/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9e55255a81270b768439c	O-RED-ENTE-070324/296

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 Version(s): 9.0					
Improper Authentication	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/cgit/hostap/commit/?id=8e6485a1bcb0baffdea9e55255a81270b768439c	O-RED-ENTE-070324/297

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**		