

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

## 16 - 30 Apr 2024

Vol. 11 No. 8

Table of Content							
Vendor	Page Number						
Application							
aditya88	online_furniture_shopping_ecommerce_website	1					
Cisco	firepower_threat_defense	2					
	firepower_threat_defense_software	154					
crushftp	crushftp	227					
Google	chrome	228					
IBM	aspera_faspex	229					
Oracle	complex_maintenance_repair_and_overhaul	230					
Operating System							
Cisco	adaptive_security_appliance_software	238					
	ios_xe	757					
Linux	linux_kernel	783					

Common Vulnerabilities and Exposures (CVE) Report						
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			Application			
Vendor: adi	itya88					
Product: on	line_furniture	_shopping	g_ecommerce_website			
Affected Ver	sion(s): 1.0					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-Apr-2024	8.8	A vulnerability was found in Kashipara Online Furniture Shopping Ecommerce Website 1.0 and classified as critical. This issue affects some unknown processing of the file prodInfo.php. The manipulation of the argument prodId leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261797 was assigned to this vulnerability. <b>CVE ID : CVE-2024- 4071</b>	N/A	A-ADI-ONLI- 030524/1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2024	5.4	A vulnerability was found in Kashipara Online Furniture Shopping Ecommerce Website 1.0. It has been classified as problematic. Affected is an unknown function of the file search.php. The manipulation of the argument txtSearch leads to cross site scripting. It is possible to launch the attack	N/A	A-ADI-ONLI- 030524/2	

0-1

1-2

2-3

**3-4 4-5** Page **1** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. VDB-261798 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2024-</b> <b>4072</b>		
Vendor: Cis	co				
Product: fir	epower_threat	_defense			
Affected Ver	sion(s): 6.2.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/3

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/4

0-1

1-2

2-3

**3-4 4-5** Page **3** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.2.3.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/5
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/6

0-1

1-2

2-3

3-4 4-5 Page **4** of **1051** 

5-6 6-7 7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges.		
			Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An		
			attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.2.3.10	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/7
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/8

0-1

1-2

2-3

**3-4 4-5** Page **6** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.11			•	

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/9
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/10

0-1

1-2

2-3

**3-4 4-5** Page **8** of **1051**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.12	2			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/11

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/12

0-1

1-2

2-3

**3-4 4-5** Page **10** of **1051** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 6.2.3.13	3	20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/13

0-1

1-2

2-33-44-5Page 11 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/14

0-1

1-2

2-33-44-5Page 12 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	<mark>sion(s): 6.2.3.1</mark> 4	ł			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/15

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/16
			This vulnerability is due to improper		

0-1

1-2

2-33-44-5Page 14 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Vers	sion(s): 6.2.3.15	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/17

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/18

0-1

1-2

2-3

**3-4 4-5** Page **16** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.16	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/19

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/20
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 18 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.2.3.17	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/21

0-1

1-2

2-33-44-5Page 19 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/22

0-1

1-2

2-3

**3-4 4-5** Page **20** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b> <b>20359</b>		
Affected Ver	sion(s): 6.2.3.18	}			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/23

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/24

0-1

1-2

2-3

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 6.2.3.2				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/25
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/26

0-1

1-2

2-33-44-5Page 23 of 1051

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges. Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			vanierability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.2.3.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/27
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/28

0-1

1-2

2-33-44-5Page 25 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
Affacted Ver	sion(s): 6.2.3.4		This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.4				

0-1

1-2

2-3

**3-4 4-5** Page **26** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/29
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/30

0-1

1-2

2-33-44-5Page 27 of 1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.5				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/31

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/32

0-1

1-2

2-3

**3-4 4-5** Page **29** of **1051** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 6.2.3.6		20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/33

0-1

1-2

2-33-44-5Page 30 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/34

0-1

1-2

 2-3
 3-4
 4-5

 Page
 31 of
 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.7				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/35

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/36

0-1

1-2

2-33-44-5Page 33 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.8				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/37

0-1

1-2

2-3

**3-4 4-5** Page **34** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/38

0-1

1-2

2-3

**3-4 4-5** Page **35** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.2.3.9				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/39

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/40
			copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 37 of 1051

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.4.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/41

0-1

1-2

2-33-44-5Page 38 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/42

0-1

1-2

2-3

**3-4 4-5** Page **39** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b> <b>20359</b>		
Affected Ver	<mark>sion(s): 6.4.0.1</mark>				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/43

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/44

0-1

1-2

2-3

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Vers	sion(s): 6.4.0.10	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/45
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/46

0-1

1-2

2-33-44-5Page 42 of 1051

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges.		
			Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An		
			attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.4.0.11	Ĺ			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/47
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/48

0-1

1-2

2-33-44-5Page 44 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.12	2	20339		

0-1

1-2

2-3

**3-4 4-5** Page **45** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/49
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/50

0-1

1-2

2-33-44-5Page 46 of 1051

7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.13	}			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/51

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/52

0-1

1-2

2-3

**3-4 4-5** Page **48** of **1051**  7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 6.4.0.14	ŀ	20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/53

0-1

1-2

2-33-44-5Page 49 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/54

0-1

1-2

2-3

**3-4 4-5** Page **50** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.15	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/55

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20353 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/56

0-1

1-2

2-33-44-5Page 52 of 1051

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.16	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/57

0-1

1-2

2-3

**3-4 4-5** Page **53** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/58

0-1

1-2

2-3

**3-4 4-5** Page **54** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.17	7		<u> </u>	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/59

0-1

1-2

2-33-44-5Page 55 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/60
			flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 56 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.4.0.2				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/61

0-1

1-2

2-33-44-5Page 57 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/62

0-1

1-2

2-3

**3-4 4-5** Page **58** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b> <b>20359</b>		
Affected Ver	sion(s): 6.4.0.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/63

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/64

0-1

1-2

2-3

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.4.0.4				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/65
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/66

0-1

1-2

2-33-44-5Page 61 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges.		
			Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An		
			attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.4.0.5				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/67
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/68

0-1

1-2

2-33-44-5Page 63 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.6				

0-1

1-2

2-3

**3-4 4-5** Page **64** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/69
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/70

0-1

1-2

2-33-44-5Page 65 of 1051

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.7				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/71

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/72

0-1

1-2

2-3

**3-4 4-5** Page **67** of **1051**  5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 6.4.0.8		20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/73

0-1

1-2

2-33-44-5Page 68 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/74

0-1

1-2

2-3

**3-44-5** Page **69** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.4.0.9				<u> </u>
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/75

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/76

0-1

1-2

2-33-44-5Page 71 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.6.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/77

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/78

0-1

1-2

2-3

**3-4 4-5** Page **73** of **1051**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.6.0.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/79

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/80
			attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 75 of 1051

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.6.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/81

0-1

1-2

2-33-44-5Page 76 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/82

0-1

1-2

2-3

**3-4 4-5** Page **77** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b> <b>20359</b>		
Affected Ver	sion(s): 6.6.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/83

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/84

0-1

1-2

2-3

**3-4 4-5** Page **79** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.6.4				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/85
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/86

0-1

1-2

2-33-44-5Page 80 of 1051

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges. Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			vanierability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

<u>6-7</u>7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.6.5				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/87
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/88

0-1

1-2

2-33-44-5Page 82 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
Affected Ver			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.6.5.1				

0-1

1-2

2-3

**3-4 4-5** Page **83** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/89
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/90

0-1

1-2

2-33-44-5Page 84 of 1051

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.6.5.2				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/91

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/92

0-1

1-2

2-3

**3-4 4-5** Page **86** of **1051**  7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability is		
			due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device		
			after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.6.7				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/93

0-1

1-2

2-3

**3-44-5** Page **87** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/94

0-1

1-2

2-3

**3-4 4-5** Page **88** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.6.7.1			L	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/95

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/96

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.7.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/97

0-1

1-2

2-3

**3-4 4-5** Page **91** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/98

0-1

1-2

2-3

**3-4 4-5** Page **92** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 6.7.0.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/99

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/100
			attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 94 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 6.7.0.2				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/101

0-1

1-2

2-33-44-5Page **95** of **1051** 

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/102

0-1

1-2

2-33-44-5Page 96 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b> <b>20359</b>		
Affected Ver	sion(s): 6.7.0.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/103

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/104

0-1

1-2

2-33-44-5Page 98 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 7.0.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/105
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/106

0-1

1-2

2-33-44-5Page 99 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges.		
			Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An		
			attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

2-33-44-5Page 100 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 7.0.0.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/107
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/108

0-1

1-2

2-33-44-5Page 101 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Vers	sion(s): 7.0.1				

0-1

1-2

2-33-44-5Page 102 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/109
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/110

0-1

1-2

2-33-44-5Page 103 of 1051

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.0.1.1				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/111

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/112

0-1

1-2

2-33-44-5Page 105 of 1051

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.0.2				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/113

0-1

1-2

2-33-44-5Page 106 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/114

0-1

1-2

2-33-44-5Page 107 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.0.2.1				I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/115

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/116

0-1

1-2

2-33-44-5Page 109 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.0.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/117

0-1

1-2

2-33-44-5Page 110 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/118

0-1

1-2

2-33-44-5Page 111 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.0.4				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/119

0-1

1-2

2-33-44-5Page 112 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/120
			flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 113 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 7.0.5				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/121

0-1

1-2

2-33-44-5Page 114 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/122

0-1

1-2

2-33-44-5Page 115 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b> <b>20359</b>		
Affected Ver	sion(s): 7.0.6				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/123

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/124

0-1

1-2

2-33-44-5Page 117 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Vers	sion(s): 7.0.6.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/125
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/126

0-1

1-2

2-33-44-5Page 118 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges.		
			Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An		
			attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 7.1.0			•	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/127
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/128

0-1

1-2

2-33-44-5Page 120 of 1051

5-6

6-7

7-8

Weakness Pu	ıblish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
Affected Version	(s).7101		This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Version	(s): 7.1.0.1				

0-1

1-2

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/129
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/130

0-1

1-2

2-33-44-5Page 122 of 1051

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.1.0.2				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/131

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/132

0-1

1-2

2-33-44-5Page 124 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.1.0.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/133

0-1

1-2

2-33-44-5Page 125 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/134

0-1

1-2

2-33-44-5Page 126 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.2.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/135

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/136

0-1

1-2

2-33-44-5Page 128 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.2.0.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/137

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/138

0-1

1-2

2-33-44-5Page 130 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.2.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/139

0-1

1-2

2-33-44-5Page 131 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/140
			flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 132 of 1051

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 7.2.2		20337		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/141

0-1

1-2

2-33-44-5Page 133 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/142

0-1

1-2

2-33-44-5Page 134 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
meeteu vel	sion(s): 7.2.3		A vulnerability in the		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/143

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/144

0-1

1-2

2-33-44-5Page 136 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 7.2.4				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/145
Improper Control of Generation	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the	https://sec.cl oudapps.cisco .com/security	A-CIS-FIRE- 030524/146

0-1

1-2

2-33-44-5Page 137 of 1051

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code			preloading of VPN	/center/conte	
('Code			clients and plug-ins and	nt/CiscoSecur	
Injection')			that has been available	ityAdvisory/ci	
			in Cisco Adaptive	sco-sa-asaftd-	
			Security Appliance	persist-rce-	
			(ASA) Software and	FLsNXF4h	
			Cisco Firepower Threat		
			Defense (FTD) Software		
			could allow an		
			authenticated, local		
			attacker to execute		
			arbitrary code with		
			root-level privileges.		
			Administrator-level		
			privileges are required		
			to exploit this		
			vulnerability.		
			This vulnerability is		
			due to improper		
			validation of a file when		
			it is read from system		
			flash memory. An		
			attacker could exploit		
			this vulnerability by		
			copying a crafted file to		
			the disk0: file system of		
			an affected device. A		
			successful exploit could		
			allow the attacker to		
			execute arbitrary code		
			on the affected device		
			after the next reload of		
			the device, which could		
			alter system behavior.		
			Because the injected		
			code could persist		
			across device reboots,		
			Cisco has raised the		
			Security Impact Rating		
			(SIR) of this advisory		
			from Medium to High.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 7.2.4.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/147
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/148

0-1

1-2

2-33-44-5Page 139 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Vers	sion(s): 7.2.5				

0-1

1-2

2-33-44-5Page 140 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/149
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/150

0-1

1-2

2-33-44-5Page 141 of 1051

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.2.5.1				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-FIRE- 030524/151

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/152

0-1

1-2

2-33-44-5Page 143 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.3.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/153

0-1

1-2

2-33-44-5Page 144 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/154

0-1

1-2

2-33-44-5Page 145 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.3.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/155

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/156
			This vulnerability is due to improper		

0-1

1-2

2-33-44-5Page 147 of 1051

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.3.1.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/157

0-1

1-2

2-3 3-4 4-5 Page **148** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/158

0-1

1-2

2-33-44-5Page 149 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 7.4.0				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/159

0-1

1-2

2-33-44-5Page 150 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/160
			flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could		

0-1

1-2

2-33-44-5Page 151 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 7.4.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	A-CIS-FIRE- 030524/161

0-1

1-2

2-33-44-5Page 152 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	A-CIS-FIRE- 030524/162

0-1

1-2

2-33-44-5Page 153 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024</b> -		
Product: fir	epower_threat	defense	20359 software		
	rsion(s): 6.2.3	_ucrense			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/163

0-1

1-2

2-33-44-5Page 154 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on the underlying Linux operating system as root.		
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 6.2.3.1		I		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/164

0-1

1-2

2-33-44-5Page 155 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as root. <b>CVE ID : CVE-2024-</b>		
			20358		
Affected Ver	sion(s): 6.2.3.10	)		L	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/165

0-1

1-2

2-33-44-5Page 156 of 1051

6-7 7-8

5-6

9-10

Affected Version(s): 6.2.3.11A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the tacker to execute arbitrary commands on the underlying the contents of a backup file to an affected device. A successful exploit could allow the tacker to execute arbitrary commands on the underlying system as root.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecurity /so-sa-asaftd- cmd-inij- ZJV8WysmA-CIS-FIRE- 030524/166Affected Version(s): 6.2.3.126.7CVE ID : CVE-2024- 20358A-CIS-FIRE- 03524/166	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an DS Command Injection')24-Apr-20246.7A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.A-CIS-FIRE- 030524/166						
Improper Neutralizat ion of Special Elements used in an injection"24-Apr-20246.7Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges are required to exploit this vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could alow the attacker to abackup file to an affected device. A successful exploit could alow the attacker to execute arbitrary commands on the underlying linux operating system as root.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- go524/166A-CIS-FIRE- 030524/166Command Injection"6.7Firepower to exploit this vulnerability exists because the contents of a backup file are improperly sanitized at restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying linux operating system as root.https://sec.cl oudapps.cisco .com/security .com/security .com/securityCVE ID : CVE-2024- 20358CVE ID : CVE-2024- 20358aa	Affected Ver	sion(s): 6.2.3.11	-		I	I
Allected Version(5). 0.2.3.12	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')			Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj-	

0-1

1-2

2-33-44-5Page 157 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/167
Affected Vers	ion(s): 6.2.3.13	;			
Improper Neutralizat ion of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-FIRE- 030524/168

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness Elements used in an OS Command ('OS Command Injection')	Publish Date	CVSSV3	Description & CVE IDavailable in Cisco ASASoftware and CiscoFirepower ThreatDefense (FTD) Softwarecould allow anauthenticated, localattacker to executearbitrary commands onthe underlyingoperating system withroot-level privileges.Administrator-levelprivileges are requiredto exploit thisvulnerability. Thisvulnerability existsbecause the contents ofa backup file areimproperly sanitized atrestore time. Anattacker could exploitthis vulnerability byrestoring a craftedbackup file to anaffected device. Asuccessful exploit couldallow the attacker toexecute arbitrarycommands on theunderlying Linuxoperating system asroot.CVE ID : CVE-2024-	Patch nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Affected Mar			20358		
	sion(s): 6.2.3.14	ł	A 1 1-11- 1-11		
Improper Neutralizat ion of Special Elements used in an OS Command	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/169

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.2.3.15	5			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/170

0-1

1-2

2-33-44-5Page 160 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.2.3.16	)			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/171

0-1

1-2

2-33-44-5Page 161 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.2.3.17	7	20358		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/172

0-1

1-2

2-33-44-5Page 162 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.		
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 6.2.3.18	3	A 1 1:1:1: : .1		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/173

0-1

1-2

2-33-44-5Page 163 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Affected Ver	sion(s): 6.2.3.2				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/174

0-1

1-2

2-33-44-5Page 164 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Affected Ver	<mark>sion(s): 6.2.3.3</mark>				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/175

0-1

1-2

2-33-44-5Page 165 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
			20358		
Affected Ver	sion(s): 6.2.3.4				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/176

0-1

1-2

**2-3** 3-4 4-5 Page **166** of **1051**  5-6

Affected Version(s): 6.2.3.5         Affected Version(s): 6.2.3.5         Affected Version(s): 6.2.3.5         A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability exists because the contents of a backup file are improperty sanitized at restore time. An attacker to execute arbitrary commands on the underlying this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Sitem as root. CVE ID : CVE-2024- 70358       A-CIS-FIRE- 00524/177	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command Injection')24-Apr-20246.7A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.A-CIS-FIRE- 030524/1770CVE ID : CVE-2024-CVE ID : CVE-2024-A						
Improper Neutralizat ion of Special Elements used in an injection')24-Apr-20246.7Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are attacker could exploit this vulnerability by restore time. An affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.A-CIS-FIRE- 030524/177A-CIS-FIRE- 030524/1770.4A-CIS-FIRE- 030524/177	Affected Ver	sion(s): 6.2.3.5			I	
Affected Version(s): 6.2.3.6	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')		6.7	Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj-	

0-1

1-2

2-33-44-5Page 167 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/178
Affected Versi	ion(s): 6.2.3.7				1
Improper Neutralizat ion of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-FIRE- 030524/179

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.2.3.8				
Improper Neutralizat ion of Special Elements used in an OS Command	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/180

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.2.3.9				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/181

0-1

1-2

2-33-44-5Page 170 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.4.0			·	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/182

0-1

1-2

2-33-44-5Page 171 of 1051

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.4.0.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/183

0-1

1-2

2-33-44-5Page 172 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Affected Ver	aion(a), ( 4.0.1(		20358		
Affected ver	<mark>sion(s): 6.4.0.10</mark>	)	A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vumerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/184

0-1

1-2

2-33-44-5Page 173 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024</b> -		
Affected Ver	sion(s): 6.4.0.11		20358		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/185

0-1

1-2

2-33-44-5Page 174 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	<mark>sion(s): 6.4.0.12</mark>	)			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/186

0-1

1-2

2-33-44-5Page 175 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
			20358		
Affected Ver	sion(s): 6.4.0.13	3			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/187

0-1

1-2

2-33-44-5Page 176 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20358		
Affected Versi	on(s): 6.4.0.14			L	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/188

0-1

1-2

2-33-44-5Page 177 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/189
	sion(s): 6.4.0.16	)			
Improper Neutralizat ion of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-FIRE- 030524/190

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness Elements used in an OS Command ('OS Command Injection')	Publish Date	CVSSV3	Description & CVE IDavailable in Cisco ASASoftware and CiscoFirepower ThreatDefense (FTD) Softwarecould allow anauthenticated, localattacker to executearbitrary commands onthe underlyingoperating system withroot-level privileges.Administrator-levelprivileges are requiredto exploit thisvulnerability. Thisvulnerability existsbecause the contents ofa backup file areimproperly sanitized atrestore time. Anattacker could exploitthis vulnerability byrestoring a craftedbackup file to anaffected device. Asuccessful exploit couldallow the attacker toexecute arbitrarycommands on theunderlying Linuxoperating system asroot.CVE ID : CVE-2024-	Patch nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.4.0.17	7	20358		
			A milnorability in the		
Improper Neutralizat ion of Special Elements used in an OS Command	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/191

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.4.0.2		·	•	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/192

0-1

1-2

**2-3** 3-4 4-5 Page **180** of **1051**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.4.0.3			·	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/193

0-1

1-2

2-33-44-5Page 181 of 1051

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.4.0.4				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/194

0-1

1-2

2-33-44-5Page 182 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Affected Mar			20358		
Affected ver	<mark>sion(s): 6.4.0.5</mark>		A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vumerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/195

0-1

1-2

2-33-44-5Page 183 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.		
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 6.4.0.6				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/196

0-1

1-2

**2-3** 3-4 4-5 Page **184** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Affected Ver	sion(s): 6.4.0.7		20330		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/197

0-1

1-2

2-33-44-5Page 185 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
			20358		
Affected Ver	sion(s): 6.4.0.8		·		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/198

0-1

1-2

**2-3** 3-4 4-5 Page **186** of **1051**  5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 6.4.0.9			L	L
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/199
	51011(3): 0.0.0				

0-1

1-2

2-33-44-5Page 187 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/200
	sion(s): 6.6.0.1				
Improper Neutralizat ion of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-FIRE- 030524/201

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.6.1		20358		
Improper Neutralizat ion of Special Elements used in an OS Command	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/202

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.6.3				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/203

0-1

1-2

2-33-44-5Page 190 of 1051

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.6.4				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/204

0-1

1-2

2-33-44-5Page 191 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 6.6.5				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/205

0-1

1-2

2-33-44-5Page 192 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 6.6.5.1		20358		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/206

0-1

1-2

2-33-44-5Page 193 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024</b> -		
Affected Ver	sion(s): 6.6.5.2		20358		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/207

0-1

1-2

2-33-44-5Page 194 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Affected Ver	sion(s): 6.6.7				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/208

0-1

1-2

2-33-44-5Page 195 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
			20358		
Affected Ver	sion(s): 6.6.7.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/209

0-1

1-2

2-3 3-4 4-5 Page **196** of **1051**  5-6

used in an OS Command ('OS Command Injection')24-Apr-20246.7vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker tont/CiscoSecur ityAdvisory/ci sco-sa-asaftd- CM-inj- ZJV8Wysm030524/21	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command (Injection')24-Apr-20246.7A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker tohttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecuri ityAdvisory/ci sco-sa-asaftd- cmd-inj-A-CIS-FIRE- 030524/21						
Improper Neutralizat ion of Special Elements used in an OS24-Apr-20246.7Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker tohttps://sec.cl oudapps.cisco .com/security dvisory/ci sco-sa-asaftd- cmd-inj-A-CIS-FIRE- 030524/21	Affected Ver	sion(s): 6.7.0		L	L	
Affected Version(s): 6.7.0.1           commands on the underlying Linux operating system as root.       CVE ID : CVE-2024- 20358	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')		6.7	Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj-	A-CIS-FIRE- 030524/210

0-1

1-2

2-33-44-5Page 197 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/211
	sion(s): 6.7.0.2				
Improper Neutralizat ion of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-FIRE- 030524/212

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Description & CVE IDavailable in Cisco ASASoftware and CiscoFirepower ThreatDefense (FTD) Softwarecould allow anauthenticated, localattacker to executearbitrary commands onthe underlyingoperating system withroot-level privileges.Administrator-levelprivileges are requiredto exploit thisvulnerability. Thisvulnerability existsbecause the contents ofa backup file areimproperly sanitized atrestore time. Anattacker could exploitthis vulnerability byrestoring a craftedbackup file to anaffected device. Asuccessful exploit couldallow the attacker toexecute arbitrarycommands on theunderlying Linuxoperating system asroot.CVE ID : CVE-2024-	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 6.7.0.3		20358		
Improper Neutralizat ion of Special Elements used in an OS Command	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/213

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 7.0.0		·		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/214

0-1

1-2

2-33-44-5Page 200 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 7.0.0.1			•	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/215

0-1

1-2

2-33-44-5Page 201 of 1051

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 7.0.1		20358		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/216

0-1

1-2

2-33-44-5Page 202 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 7.0.1.1		20358		
			A vulnerability in the Cisco Adaptive Security		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/217

0-1

1-2

2-33-44-5Page 203 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.		
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 7.0.2			I	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/218

0-1

1-2

2-33-44-5Page 204 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Affected Ver	sion(s): 7.0.2.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/219

0-1

1-2

2-33-44-5Page 205 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying Linux operating system as root.		
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 7.0.3				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/220

0-1

1-2

2-33-44-5Page 206 of 1051

6-7 7-8

5-6

		CVE ID : CVE-2024- 20358					
Affected Version(s): 7.0.4							
Improper Neutralizat ion of Special Elements used in an ('OS Command Injection') Affected Version(s): 7.0.5	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/221			

0-1

1-2

2-33-44-5Page 207 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/222
	sion(s): 7.0.6				
Improper Neutralizat ion of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-FIRE- 030524/223

0-1

1-2

**2-3** 3-4 4-5 Page **208** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		CVSSV3	Description & CVE IDavailable in Cisco ASASoftware and CiscoFirepower ThreatDefense (FTD) Softwarecould allow anauthenticated, localattacker to executearbitrary commands onthe underlyingoperating system withroot-level privileges.Administrator-levelprivileges are requiredto exploit thisvulnerability. Thisvulnerability existsbecause the contents ofa backup file areimproperly sanitized atrestore time. Anattacker could exploitthis vulnerability byrestoring a craftedbackup file to anaffected device. Asuccessful exploit couldallow the attacker toexecute arbitrarycommands on theunderlying Linuxoperating system asroot.CVE ID : CVE-2024-	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 7.0.6.1		20358		
Improper Neutralizat ion of Special Elements used in an OS Command	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/224

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 7.1.0		·		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/225

0-1

1-2

2-33-44-5Page 210 of 1051

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 7.1.0.1			·	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/226

0-1

1-2

2-33-44-5Page 211 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 7.1.0.2				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/227

0-1

1-2

2-33-44-5Page 212 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s), 7102		20358		
Anected ver	sion(s): 7.1.0.3		A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/228

0-1

1-2

2-33-44-5Page 213 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.		
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 7.2.0			I	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/229

0-1

1-2

2-33-44-5Page 214 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Affected Ver	sion(s): 7.2.0.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/230

0-1

1-2

2-33-44-5Page 215 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying Linux operating system as root.		
			CVE ID : CVE-2024- 20358		
Affected Ver	sion(s): 7.2.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/231

0-1

1-2

2-33-44-5Page 216 of 1051

7-8

6-7

5-6

9-10

Affected Version(s): 7.2.2CVE ID : CVE-2024-20358Affected Version(s): 7.2.2A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying linux operating system as root.A-CIS-FIRE- 030524/232	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an injection")24-Apr-20246.7A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability exists because the contents of a backup file are improper time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying linux operating system as root.https://sec.cl oudapps.cisco com/security /center/conte nt/CiscoSecur ityAdvisory/ci so-sa-asafd- adfie to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.https://sec.cl oudapps.cisco execute arbitrary commands on the underlying Linux operating system as root.https://sec.clhttps://sec.cl03CVE ID : CVE-2024-CVE ID : CVE-2024-Https://sec.clImproved autocheckerImproved autochecker						
Improper Neutralization of Special Elements used in an (OS Command (POS Command Injection')24-Apr-20246.7Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability exists because the contents of a backup file an arfsect et device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying linux operating system as root.https://sec.cl oudaps.cisco .com/security /center/conte nt/CiscoSecuri ty/dvisory/ci Sto-sa-asafd- cmd-inj- ZIV8WysmA-CIS-FIRE- 030524/232Improper Secure Command (OS Command (OS Command (OS Command (DS Command (DS Command (DS Command (DS Command (DS Command (DS Command (DS Command (DS COMMAND (CS COMMAND (CS COMMAND (DS COMMANDD (DS COMMANDD (DS COMMANDD (DS (	Affected Ver	sion(s): 7.2.2			I	L
Affected Version(s): 7.2.3	Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')		6.7	Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj-	

0-1

1-2

2-33-44-5Page 217 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/233
	sion(s): 7.2.4				
Improper Neutralizat ion of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-FIRE- 030524/234

0-1

1-2

2-33-44-5Page 218 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 7.2.4.1		20000		
Improper Neutralizat ion of Special Elements used in an OS Command	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	A-CIS-FIRE- 030524/235

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	cmd-inj- ZJV8Wysm	
Affected Ver	sion(s): 7.2.5				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/236

0-1

1-2

2-33-44-5Page 220 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 7.2.5.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/237

0-1

1-2

2-33-44-5Page 221 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Affected Ver	sion(s): 7.3.0		20358		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/238

0-1

1-2

2-33-44-5Page 222 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Affected Ver	aion(a), 7.2.1		20358		
Allected ver	sion(s): 7.3.1		A vulnerability in the		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/239

0-1

1-2

2-33-44-5Page 223 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024</b> -		
Affected Ver	sion(s): 7.3.1.1		20358		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/240

0-1

1-2

2-33-44-5Page 224 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Affected Ver	sion(s): 7.4.0				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/241

0-1

1-2

2-33-44-5Page 225 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
			20358		
Affected Ver	sion(s): 7.4.1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	A-CIS-FIRE- 030524/242

0-1

1-2

2-33-44-5Page 226 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20358		
Vendor: cru	ishftp				
Product: cr	ushftp				
Affected Ver	sion(s): From (i	ncluding)	10.0.0 Up to (excluding) 1	0.7.1	
Improper Control of Generation of Code ('Code Injection')	22-Apr-2024	10	A server side template injection vulnerability in CrushFTP in all versions before 10.7.1 and 11.1.0 on all platforms allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server.	https://www. crushftp.com/ crush10wiki/ Wiki.jsp?page =Update, https://www. crushftp.com/ crush11wiki/ Wiki.jsp?page =Update, https://www. reddit.com/r/ cybersecurity /comments/1 c850i2/all_ve rsions_of_crus h_ftp_are_vuln erable/	A-CRU-CRUS- 030524/243
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	4040 11.0.0 Up to (excluding) 1	1.1.0	
Improper Control of Generation of Code ('Code Injection')	22-Apr-2024	10	A server side template injection vulnerability in CrushFTP in all versions before 10.7.1 and 11.1.0 on all platforms allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server.	https://www. crushftp.com/ crush10wiki/ Wiki.jsp?page =Update, https://www. crushftp.com/ crush11wiki/ Wiki.jsp?page =Update, https://www. reddit.com/r/ cybersecurity /comments/1 c850i2/all_ve rsions_of_crus	A-CRU-CRUS- 030524/244

0-1

1-2

2-33-44-5Page 227 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2024- 4040	h_ftp_are_vuln erable/		
Vendor: Go	<u> </u>					
Product: ch		<u> </u>				
Affected Ver	sion(s): * Up to	(excluding	g) 124.0.6367.60			
Use After Free	17-Apr-2024	8.8	Use after free in Downloads in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) <b>CVE ID : CVE-2024-</b> <b>3834</b>	https://chro mereleases.go ogleblog.com/ 2024/04/stab le-channel- update-for- desktop_16.ht ml	A-GOO- CHRO- 030524/245	
Use After Free	17-Apr-2024	8.8	Use after free in QUIC in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) CVE ID : CVE-2024- 3837	https://chro mereleases.go ogleblog.com/ 2024/04/stab le-channel- update-for- desktop_16.ht ml	A-GOO- CHRO- 030524/246	
Out-of- bounds Read	17-Apr-2024	6.5	Out of bounds read in Fonts in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	https://chro mereleases.go ogleblog.com/ 2024/04/stab le-channel- update-for- desktop_16.ht ml	A-GOO- CHRO- 030524/247	
CVSS Section		1 2 3		67 70	<u> 20 040</u>	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 228 of 1051						

Page 228 of 1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 3839		
N/A	17-Apr-2024	5.5	Inappropriate implementation in Autofill in Google Chrome prior to 124.0.6367.60 allowed an attacker who convinced a user to install a malicious app to perform UI spoofing via a crafted app. (Chromium security severity: Medium)	https://chro mereleases.go ogleblog.com/ 2024/04/stab le-channel- update-for- desktop_16.ht ml	A-GOO- CHRO- 030524/248
			CVE ID : CVE-2024- 3838		
Vendor: IBN	1				
	pera_faspex				
Affected Ver	sion(s): From (i	ncluding)	5.0.0 Up to (including) 5.0	.7	
N/A	19-Apr-2024	6.5	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a user to cause a denial of service due to missing API rate limiting. IBM X-Force ID: 248533. <b>CVE ID : CVE-2023-</b> <b>27279</b>	https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 248533, https://www. ibm.com/sup port/pages/n ode/7148632	A-IBM-ASPE- 030524/249
Inadequate Encryption Strength	19-Apr-2024	5.5	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain sensitive information due to weaker than expected security. IBM X-Force ID: 236452. <b>CVE ID : CVE-2022-</b> <b>40745</b>	https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 236452, https://www. ibm.com/sup port/pages/n ode/7148632	A-IBM-ASPE- 030524/250

0-1

1-2

2-3 3-4 4-5 Page 229 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	19-Apr-2024	4.4	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain or modify sensitive information due to improper encryption of certain data. IBM X-Force ID: 259672. <b>CVE ID : CVE-2023-</b> <b>37397</b>	https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 259672, https://www. ibm.com/sup port/pages/n ode/7148632	A-IBM-ASPE- 030524/251
Vendor: Ora	acle				
Product: co	mplex_mainte	nance_rep	oair_and_overhaul		
Affected Ver	sion(s): From (i	ncluding)	12.2.3 Up to (including) 12	2.2.13	
N/A	16-Apr-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected are 12.2.3- 12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly	https://www. oracle.com/se curity- alerts/cpuapr 2024.html	A-ORA- COMP- 030524/252

0-1

1-2

2-33-44-5Page 230 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:R/S:C/C:L/I:L/A :N).		
N/A	16-Apr-2024	6.1	21026 Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected are 12.2.3- 12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle	https://www. oracle.com/se curity- alerts/cpuapr 2024.html	A-ORA- COMP- 030524/253

0-1

1-2

2-33-44-5Page 231 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:R/S:C/C:L/I:L/A :N). <b>CVE ID : CVE-2024- 21027</b>		
N/A	16-Apr-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product	https://www. oracle.com/se curity-	A-ORA- COMP- 030524/254

0-1

1-2

5-6

6-7

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		of Oracle E-Business	alerts/cpuapr	
		Suite (component:	2024.html	
		LOV). Supported		
		affected are 12.2.3-		
		12.2.13. Easily		
		-		
		-		
		-		
		_		
		-		
		•		
		-		
		_		
		_		
		_		
		-		
		-		
		-		
		-		
		-		
		and Overhaul accessible		
		data. CVSS 3.1 Base		
		Score 6.1		
	Publish Date	Publish Date CVSSv3	of Oracle E-BusinessSuite (component: LOV). Supported versions that are affected are 12.2.3- 12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex	of Oracle E-Business Suite (component: LOV). Supported versions that are affected are 12.2.3- 12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data cCVSS 3.1 Base Score 6.1alerts/cpuapr 2024.html

0-1

1-2

2-33-44-5Page 233 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:R/S:C/C:L/I:L/A :N). CVE ID : CVE-2024-		
			21028		
N/A	16-Apr-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected are 12.2.3- 12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	https://www. oracle.com/se curity- alerts/cpuapr 2024.html	A-ORA- COMP- 030524/255

0-1

1-2

2-33-44-5Page 234 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:R/S:C/C:L/I:L/A :N). <b>CVE ID : CVE-2024- 21029</b>		
N/A	16-Apr-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected are 12.2.3- 12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in	https://www. oracle.com/se curity- alerts/cpuapr 2024.html	A-ORA- COMP- 030524/256

0-1

1-2

2-33-44-5Page 235 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:R/S:C/C:L/I:L/A :N). <b>CVE ID : CVE-2024- 21030</b>		
N/A	16-Apr-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected are 12.2.3- 12.2.13. Easily exploitable vulnerability allows	https://www. oracle.com/se curity- alerts/cpuapr 2024.html	A-ORA- COMP- 030524/257

0-1

1-2

2-3 3-4 4-5 Page 236 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated		
			attacker with network		
			access via HTTP to		
			compromise Oracle		
			Complex Maintenance,		
			Repair, and Overhaul.		
			Successful attacks		
			require human		
			interaction from a		
			person other than the		
			attacker and while the		
			vulnerability is in		
			Oracle Complex		
			Maintenance, Repair,		
			and Overhaul, attacks		
			may significantly		
			impact additional		
			products (scope		
			change). Successful		
			attacks of this		
			vulnerability can result		
			in unauthorized		
			update, insert or delete		
			access to some of		
			Oracle Complex		
			Maintenance, Repair,		
			and Overhaul accessible		
			data as well as		
			unauthorized read		
			access to a subset of		
			Oracle Complex		
			Maintenance, Repair,		
			and Overhaul accessible		
			data. CVSS 3.1 Base		
			Score 6.1		
			(Confidentiality and		
			Integrity impacts).		
			CVSS Vector:		
			(CVSS:3.1/AV:N/AC:L/P		
			R:N/UI:R/S:C/C:L/I:L/A		
			:N).		
			CVE ID : CVE-2024-		
			21031		
			21031		

0-1

1-2

2-33-44-5Page 237 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Operating System		
Vendor: Cise	со				
Product: ad	aptive_security	y_applian	ce_software		
Affected Ver	sion(s): 9.12.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/258
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/259

0-1

1-2

2-33-44-5Page 238 of 1051

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/260

0-1

1-2

2-33-44-5Page 239 of 1051

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.1.2	2	20337		
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/261

0-1

1-2

2-33-44-5Page 240 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/262

0-1

1-2

2-33-44-5Page 241 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/263

0-1

1-2

2-33-44-5Page 242 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.1.3	3		L	L
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/264

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/265

0-1

1-2

2-33-44-5Page 244 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
			20358 A vulnerability in a legacy capability that		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/266
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 245 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.2				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/267

0-1

1-2

2-3 3-4 4-5 Page 246 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/268

0-1

1-2

2-33-44-5Page 247 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as root.		
			CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/269

0-1

1-2

2-33-44-5Page 248 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 9.12.2.1	L			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/270

0-1

1-2

2-33-44-5Page 249 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/271
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/272

0-1

1-2

2-3 3-4 4-5 Page 250 of 1051 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 251 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): 9.12.2.4							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/273			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/274			

0-1

1-2

2-33-44-5Page 252 of 1051

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/275

0-1

1-2

2-33-44-5Page 253 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.12.2.5	5	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	0-CIS-ADAP- 030524/276

0-1

1-2

2-33-44-5Page 254 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/277

0-1

1-2

2-33-44-5Page 255 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/278

0-1

1-2

2-33-44-5Page 256 of 1051

5-6

6-7

7-8

Loop with Unreachable c Exit Condition24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the day ce to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl outgaps.cisco .com/security /consecurity /consecurity /consecurity Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl outgaps.cisco .com/security /conter/conten nt/CiscoSecurity Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl outgaps.cisco .com/security Agpliance (ASA) Software and Cisco Software an	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.12.2.920359InstanceAffected Version(s): 9.12.2.9A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security 0-CIS-ADAP- 030524/279				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD20-CIS-ADAP- 030524/279						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci S030524/279O-CIS-ADAP- 030524/279	Affected Ver	sion(s): 9.12.2.9	)			
	Unreachabl e Exit Condition ('Infinite	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	

0-1

1-2

2-33-44-5Page 257 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/280

0-1

1-2

**2-3** 3-4 4-5 Page **258** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/281

0-1

1-2

2-33-44-5Page 259 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.12.3				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/282

0-1

1-2

2-33-44-5Page 260 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/283

0-1

1-2

2-33-44-5Page 261 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/284

0-1

1-2

2-33-44-5Page 262 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.12.3.1	2			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/285
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/286

0-1

1-2

2-33-44-5Page 263 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/287

0-1

1-2

2-33-44-5Page 264 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.3.2	2	<u> </u>		
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/288

0-1

1-2

2-33-44-5Page 265 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/289

0-1

1-2

2-33-44-5Page 266 of 1051

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/290

0-1

1-2

2-33-44-5Page 267 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.3.7	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/291

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/292

0-1

1-2

2-33-44-5Page 269 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/293
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 270 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.3.9	)	20337		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/294

0-1

1-2

2-33-44-5Page 271 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/295

0-1

1-2

2-33-44-5Page 272 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/296

0-1

1-2

2-33-44-5Page 273 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 9.12.4			1	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/297

0-1

1-2

2-33-44-5Page 274 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/298
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/299

0-1

1-2

2-33-44-5Page 275 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 276 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.12.4.1	10			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/300
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/301

0-1

1-2

2-33-44-5Page 277 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/302

0-1

1-2

2-33-44-5Page 278 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.12.4.1	13	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/303

0-1

1-2

2-33-44-5Page 279 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/304

0-1

1-2

**2-3** 3-4 4-5 Page **280** of **1051**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/305

0-1

1-2

2-33-44-5Page 281 of 1051

5-6

6-7

7-8 8-9

1 /4-Apr-2024 86	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.12.4.18A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security 0-CIS-ADAP- 030524/306				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecurity 030524/306						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur tiyAdvisory/ci Software and Cisco oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci Software and Cisco Software and Cisco Defense (FTD) Software remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci Software and Cisco .com/security /center/conte nt/CiscoSecur Software attacker to Sco-sa-asaftd- Websrvs-dos- X8gNucD20-CIS-ADAP- 030524/306	Affected Ver	sion(s): 9.12.4.1	8			
This vulnerability is	Loop with Unreachabl e Exit Condition ('Infinite			management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	O-CIS-ADAP- 030524/306

0-1

1-2

2-33-44-5Page 282 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/307

0-1

1-2

2-33-44-5Page 283 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/308

0-1

1-2

**2-3** 3-4 4-5 Page **284** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.12.4.2	2			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/309

0-1

1-2

2-33-44-5Page 285 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/310

0-1

1-2

**2-3** 3-4 4-5 Page **286** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/311

0-1

1-2

2-33-44-5Page 287 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.12.4.2	24			I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/312
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/313

0-1

1-2

**2-3** 3-4 4-5 Page **288** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/314

0-1

1-2

**2-3** 3-4 4-5 Page **289** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.2	26			
Loop with			A vulnerability in the	https://sec.cl	
Unreachabl e Exit Condition	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security	oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/315

0-1

1-2

**2-3** 3-4 4-5 Page **290** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/316

0-1

1-2

2-33-44-5Page 291 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/317

0-1

1-2

2-33-44-5Page 292 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.2	29		I	I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/318

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	CVE ID : CVE-2024- 20353 A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/319

0-1

1-2

2-3 3-4 4-5 Page 294 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/320
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 295 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.3	30	20007		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/321

0-1

1-2

2-3 3-4 4-5 Page 296 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/322

0-1

1-2

2-33-44-5Page 297 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/323

0-1

1-2

**2-3** 3-4 4-5 Page **298** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 9.12.4.3	35			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/324

0-1

1-2

2-3 3-4 4-5 Page 299 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/325
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/326

0-1

1-2

2-33-44-5Page 300 of 1051

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 301 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.12.4.3	37			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/327
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/328

0-1

1-2

2-33-44-5Page 302 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/329

0-1

1-2

2-33-44-5Page 303 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.12.4.3	88	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/330

0-1

1-2

2-33-44-5Page 304 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/331

0-1

1-2

2-33-44-5Page 305 of 1051

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/332

0-1

1-2

2-3 3-4 4-5 Page **306** of **1051**  5-6

6-7

1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.12.4.39A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudaps.cisco .com/security 0-CIS-ADAP 030524/333				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci Software adaptive Security oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci Software Software Software Software Software adaptive Security Defense (FTD) Software sco-sa-asaftd- websrvs-dos- X8gNucD20-CIS-ADAP 030524/333						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Defense (FTD) Software unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudaps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci X8gNucD2O-CIS-ADAP 030524/333	Affected Ver	sion(s): 9.12.4.3	39			
This vulnerability is	Unreachabl e Exit Condition ('Infinite	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	0-CIS-ADAP- 030524/333

0-1

1-2

2-33-44-5Page 307 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/334

0-1

1-2

**2-3** 3-4 4-5 Page **308** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/335

0-1

1-2

**2-3** 3-4 4-5 Page **309** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.12.4.4	ļ.			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/336

0-1

1-2

2-33-44-5Page 310 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/337

0-1

1-2

2-33-44-5Page 311 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/338

0-1

1-2

2-33-44-5Page 312 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.12.4.</mark> 4	-0			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/339
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/340

0-1

1-2

2-33-44-5Page 313 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/341

0-1

1-2

2-33-44-5Page 314 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.4	1	20337		
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/342

0-1

1-2

2-33-44-5Page 315 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/343

0-1

1-2

2-33-44-5Page 316 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/344

0-1

1-2

2-33-44-5Page 317 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.4	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/345

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/346

0-1

1-2

2-33-44-5Page **319** of **1051** 

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/347
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 320 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.4	8			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/348

0-1

1-2

2-33-44-5Page 321 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/349

0-1

1-2

2-33-44-5Page 322 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. <b>CVE ID : CVE-2024-</b>		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/350

0-1

1-2

2-33-44-5Page 323 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.12.4.5</mark>	50			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/351

0-1

1-2

2-33-44-5Page 324 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/352
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/353

0-1

1-2

2-33-44-5Page 325 of 1051

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 326 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.12.4.5	52			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/354
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/355

0-1

1-2

2-33-44-5Page 327 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/356

0-1

1-2

**2-3** 3-4 4-5 Page **328** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.12.4.5	54	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/357

0-1

1-2

2-33-44-5Page 329 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/358

0-1

1-2

2-33-44-5Page 330 of 1051

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/359

0-1

1-2

2-33-44-5Page 331 of 1051

5-6

6-7

7-8 8-9

0-1

1-2

2-33-44-5Page 332 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/361

0-1

1-2

2-33-44-5Page 333 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/362

0-1

1-2

2-33-44-5Page 334 of 1051

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.12.4.5</mark>	56			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/363

0-1

1-2

2-33-44-5Page 335 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/364

0-1

1-2

2-33-44-5Page 336 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/365

0-1

1-2

2-33-44-5Page 337 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.12.4.5	58			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/366
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/367

0-1

1-2

**2-3** 3-4 4-5 Page **338** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/368

0-1

1-2

2-33-44-5Page 339 of 1051

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.6	52			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/369

0-1

1-2

**2-3** 3-4 4-5 Page **340** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/370

0-1

1-2

2-33-44-5Page 341 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/371

0-1

1-2

2-33-44-5Page 342 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.6	55			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/372

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	CVE ID : CVE-2024- 20353 A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/373

0-1

1-2

**2-3** 3-4 4-5 Page **344** of **1051**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/374
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 345 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.12.4.7	7	20337		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/375

0-1

1-2

2-3 3-4 4-5 Page **346** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/376

0-1

1-2

2-33-44-5Page 347 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/377

0-1

1-2

2-3 3-4 4-5 Page **348** of **1051**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.12.4.8	}			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/378

0-1

1-2

2-3 3-4 4-5 Page **349** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/379
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/380

0-1

1-2

**2-3** 3-4 4-5 Page **350** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 351 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.14.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/381
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/382

0-1

1-2

2-33-44-5Page 352 of 1051

5-6

6-7

8-9

7-8

-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/383

0-1

1-2

2-33-44-5Page 353 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.14.1.1	10	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/384

0-1

1-2

2-33-44-5Page 354 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/385

0-1

1-2

2-33-44-5Page 355 of 1051

5-6

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/386

0-1

1-2

2-3 3-4 4-5 Page **356** of **1051**  5-6

6-7

7-8

0-1

1-2

2-33-44-5Page 357 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/388

0-1

1-2

**2-3** 3-4 4-5 Page **358** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/389

0-1

1-2

2-33-44-5Page 359 of 1051

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.14.1.1	9			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/390

0-1

1-2

2-33-44-5Page 360 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/391

0-1

1-2

2-33-44-5Page 361 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/392

0-1

1-2

2-33-44-5Page 362 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Vers	sion(s): 9.14.1.3	30			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/393
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/394

0-1

1-2

2-33-44-5Page 363 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/395

0-1

1-2

**2-3** 3-4 4-5 Page **364** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.1.6	5		<u> </u>	
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/396

0-1

1-2

2-33-44-5Page 365 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/397

0-1

1-2

2-3 3-4 4-5 Page **366** of **1051**  8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/398

0-1

1-2

2-33-44-5Page 367 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.2				<u> </u>
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/399

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/400

0-1

1-2

**2-3** 3-4 4-5 Page **369** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/401
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 370 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.2.1	3			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/402

0-1

1-2

2-33-44-5Page 371 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/403

0-1

1-2

2-33-44-5Page 372 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/404

0-1

1-2

2-33-44-5Page 373 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.14.2.</mark> 1	15			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/405

0-1

1-2

2-33-44-5Page 374 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/406
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/407

0-1

1-2

2-3 3-4 4-5 Page 375 of 1051 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 376 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): 9.14.2.4								
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/408				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/409				

0-1

1-2

2-33-44-5Page 377 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/410

0-1

1-2

2-33-44-5Page 378 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.14.2.8	3	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/411

0-1

1-2

2-33-44-5Page 379 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/412

0-1

1-2

**2-3** 3-4 4-5 Page **380** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/413

0-1

1-2

2-33-44-5Page 381 of 1051

5-6

6-7

7-8 8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
		20359		
sion(s): 9.14.3		<u> </u>	I	
24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/414
	sion(s): 9.14.3	sion(s): 9.14.3	24-Apr-2024Image: construct of the construction of the constr	24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to esservice (DoS) condition.Https://sec.cl outpane.24-Apr-20248.6A vulnerability is

0-1

1-2

2-33-44-5Page 382 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/415

0-1

1-2

2-33-44-5Page 383 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/416

0-1

1-2

**2-3** 3-4 4-5 Page **384** of **1051**  7-8

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.14.3.1	_			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/417

0-1

1-2

2-33-44-5Page 385 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/418

0-1

1-2

**2-3** 3-4 4-5 Page **386** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/419

0-1

1-2

2-33-44-5Page 387 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.14.3.1	.1			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/420
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/421

0-1

1-2

**2-3** 3-4 4-5 Page **388** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/422

0-1

1-2

**2-3** 3-4 4-5 Page **389** of **1051**  5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.3.1	13			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/423

0-1

1-2

**2-3** 3-4 4-5 Page **390** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/424

0-1

1-2

2-33-44-5Page 391 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/425

0-1

1-2

2-33-44-5Page 392 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.3.1	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/426

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/427

0-1

1-2

**2-3** 3-4 4-5 Page **394** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> <b>20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/428
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 395 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.3.1	8			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/429

0-1

1-2

2-3 3-4 4-5 Page **396** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/430

0-1

1-2

2-33-44-5Page 397 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/431

0-1

1-2

**2-3** 3-4 4-5 Page **398** of **1051**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.14.3.9	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/432

0-1

1-2

**2-3** 3-4 4-5 Page **399** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/433
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/434

0-1

1-2

**2-3** 3-4 4-5 Page **400** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 401 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.14.4				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/435
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/436

0-1

1-2

2-33-44-5Page 402 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/437

0-1

1-2

2-33-44-5Page 403 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.14.4.1	.2	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	0-CIS-ADAP- 030524/438

0-1

1-2

2-33-44-5Page 404 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/439

0-1

1-2

2-33-44-5Page 405 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/440

0-1

1-2

2-3 3-4 4-5 Page **406** of **1051**  5-6

6-7

It is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVF ID : CVF-2024- 20359https://sec.cl oudpaps.cisco .cm/security Appliance (ASA) Software and Cisco Firepower Threat Defines (FTD) Software could allow an unauthenticated, renote attacker to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudpaps.cisco .com/security /conter/conte nt/CiscoSecurityAdvisory/ci so-CIS-ADAP- 0:0524/441	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.14.4.13Affected Version(s): 9.14.4.13Affected Version(s): 9.14.4.13A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofLoop ')				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software out allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci Software asgNucD20-CIS-ADAP- 030524/441						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur 0-CIS-ADAP- 030524/441	Affected Ver	sion(s): 9.14.4.1	3		<u> </u>	
This vulnerability is	Unreachabl e Exit Condition ('Infinite	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	

0-1

1-2

2-33-44-5Page 407 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/442

0-1

1-2

**2-3** 3-4 4-5 Page **408** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/443

0-1

1-2

**2-3** 3-4 4-5 Page **409** of **1051**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.14.4.1</mark>	.4			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/444

0-1

1-2

2-33-44-5Page 410 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/445

0-1

1-2

2-33-44-5Page 411 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/446

0-1

1-2

2-33-44-5Page 412 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.14.4.1</mark>	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/447
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/448

0-1

1-2

2-33-44-5Page 413 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/449

0-1

1-2

2-33-44-5Page 414 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.4.1	.7	<u> </u>		
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/450

0-1

1-2

2-33-44-5Page 415 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/451

0-1

1-2

2-33-44-5Page 416 of 1051

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/452

0-1

1-2

2-33-44-5Page 417 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.4.2	22			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/453

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/454

0-1

1-2

2-33-44-5Page 419 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/455
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 420 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.14.4.2	23			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/456

0-1

1-2

2-33-44-5Page 421 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/457

0-1

1-2

2-33-44-5Page 422 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/458

0-1

1-2

2-33-44-5Page 423 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.14.4.6	j			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/459

0-1

1-2

2-33-44-5Page 424 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/460
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/461

0-1

1-2

2-3 3-4 4-5 Page 425 of 1051 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 426 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): 9.14.4.7								
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/462				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/463				

0-1

1-2

2-33-44-5Page 427 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/464

0-1

1-2

**2-3** 3-4 4-5 Page **428** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.15.1		CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/465

0-1

1-2

2-33-44-5Page 429 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/466

0-1

1-2

2-33-44-5Page 430 of 1051

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/467

0-1

1-2

2-33-44-5Page 431 of 1051

5-6

6-7

0-1

1-2

2-33-44-5Page 432 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/469

0-1

1-2

2-33-44-5Page 433 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/470

0-1

1-2

2-33-44-5Page 434 of 1051

7-8

6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.15.1.1	10			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/471

0-1

1-2

2-33-44-5Page 435 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/472

0-1

1-2

2-3 3-4 4-5 Page **436** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/473

0-1

1-2

2-33-44-5Page 437 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.15.1.1</mark>	.5			I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/474
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/475

0-1

1-2

2-3 3-4 4-5 Page **438** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/476

0-1

1-2

2-33-44-5Page 439 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.				
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>				
Affected Vers	Affected Version(s): 9.15.1.16						
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/477		

0-1

1-2

**2-3** 3-4 4-5 Page **440** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/478

0-1

1-2

2-33-44-5Page 441 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/479

0-1

1-2

2-33-44-5Page 442 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.15.1.1	7		I	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/480

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/481

0-1

1-2

**2-3** 3-4 4-5 Page **444** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/482
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 445 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 9.15.1.2	21	20359		
			A vulnerability in the		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/483

0-1

1-2

2-3 3-4 4-5 Page **446** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/484

0-1

1-2

2-33-44-5Page 447 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/485

0-1

1-2

2-3 3-4 4-5 Page 448 of 1051 5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.15.1.7	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/486

0-1

1-2

2-3 3-4 4-5 Page **449** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/487
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/488

0-1

1-2

**2-3** 3-4 4-5 Page **450** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 451 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): 9.16.1								
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/489				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/490				

0-1

1-2

2-33-44-5Page 452 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/491

0-1

1-2

2-33-44-5Page 453 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.16.1.2	28	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/492

0-1

1-2

2-33-44-5Page 454 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/493

0-1

1-2

2-33-44-5Page 455 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/494

0-1

1-2

2-3 3-4 4-5 Page **456** of **1051**  5-6

6-7

0-1

1-2

2-33-44-5Page 457 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/496

0-1

1-2

**2-3** 3-4 4-5 Page **458** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/497

0-1

1-2

2-33-44-5Page 459 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.16.2.1	.1			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/498

0-1

1-2

2-33-44-5Page 460 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/499

0-1

1-2

2-33-44-5Page 461 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/500

0-1

1-2

2-33-44-5Page 462 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.16.2.1</mark>	3			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/501
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/502

0-1

1-2

2-33-44-5Page 463 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/503

0-1

1-2

**2-3** 3-4 4-5 Page **464** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.				
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>				
Affected Ver	Affected Version(s): 9.16.2.14						
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/504		

0-1

1-2

2-33-44-5Page 465 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/505

0-1

1-2

**2-3** 3-4 4-5 Page **466** of **1051**  6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/506

0-1

1-2

2-3 3-4 4-5 Page **467** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.16.2.3	}			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/507

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/508

0-1

1-2

2-3 3-4 4-5 Page **469** of **1051**  6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/509
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 470 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.16.2.7	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/510

0-1

1-2

2-33-44-5Page 471 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/511

0-1

1-2

2-33-44-5Page 472 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/512

0-1

1-2

2-33-44-5Page 473 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.16.3		L		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/513

0-1

1-2

2-33-44-5Page 474 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/514
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/515

0-1

1-2

2-33-44-5Page 475 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 476 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): 9.16.3.14							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/516		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/517		

0-1

1-2

2-33-44-5Page 477 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/518

0-1

1-2

2-33-44-5Page 478 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.16.3.1	15	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/519

0-1

1-2

2-33-44-5Page 479 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/520

0-1

1-2

**2-3** 3-4 4-5 Page **480** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/521

0-1

1-2

2-33-44-5Page 481 of 1051

5-6

6-7

Loop with Unreachable E Kit Condition24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an adultation or service (DoS) condition.https://sec.cl oudpus. o-CIS-ADAP- 0-CIS-ADAP- 0-30524/522Loop vith Unreachable e Fxit Condition24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an and and vehance0-CIS-ADAP- 030524/5220-CIS-ADAP- (30524/5228.60-CIS-ADAP- (30524/522	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.16.3.1920359Image: Constraint of the service of the se				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecuri ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD20-CIS-ADAP- 030524/522						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD20-CIS-ADAP- 030524/522	Affected Vers	sion(s): 9.16.3.1	9			
This vulnerability is	Unreachabl e Exit Condition ('Infinite	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	

0-1

1-2

2-33-44-5Page 482 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/523

0-1

1-2

2-33-44-5Page 483 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/524

0-1

1-2

**2-3** 3-4 4-5 Page **484** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.16.3.2	23			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/525

0-1

1-2

2-33-44-5Page 485 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/526

0-1

1-2

**2-3** 3-4 4-5 Page **486** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/527

0-1

1-2

**2-3** 3-4 4-5 Page **487** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.16.3.3	3			I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/528
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/529

0-1

1-2

**2-3** 3-4 4-5 Page **488** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/530

0-1

1-2

**2-3** 3-4 4-5 Page **489** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.16.4				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/531

0-1

1-2

**2-3** 3-4 4-5 Page **490** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/532

0-1

1-2

2-33-44-5Page 491 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/533

0-1

1-2

2-33-44-5Page 492 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.16.4.1	4			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/534

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/535

0-1

1-2

**2-3** 3-4 4-5 Page **494** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/536
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 495 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.16.4.1	8			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/537

0-1

1-2

2-3 3-4 4-5 Page **496** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/538

0-1

1-2

2-33-44-5Page 497 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as root.		
			CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/539

0-1

1-2

2-3 3-4 4-5 Page **498** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.16.4.1	19			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/540

0-1

1-2

2-3 3-4 4-5 Page **499** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/541
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/542

0-1

1-2

**2-3** 3-4 4-5 Page **500** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 501 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): 9.16.4.27							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/543			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/544			

0-1

1-2

2-33-44-5Page 502 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/545

0-1

1-2

2-33-44-5Page 503 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.16.4.3	38	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/546

0-1

1-2

2-33-44-5Page 504 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/547

0-1

1-2

2-33-44-5Page 505 of 1051

7-8

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/548

0-1

1-2

**2-3** 3-4 4-5 Page **506** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.16.4.3	39	I	I	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/549
			This vulnerability is due to incomplete error		

0-1

1-2

2-33-44-5Page 507 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/550

0-1

1-2

**2-3** 3-4 4-5 Page **508** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/551

0-1

1-2

**2-3** 3-4 4-5 Page **509** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.16.4.4	2			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/552

0-1

1-2

2-33-44-5Page 510 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/553

0-1

1-2

2-33-44-5Page 511 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/554

0-1

1-2

2-33-44-5Page 512 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Vers	<mark>sion(s): 9.16.4.4</mark>	8			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/555
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/556

0-1

1-2

2-33-44-5Page 513 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/557

0-1

1-2

2-33-44-5Page 514 of 1051

5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.16.4.5	55			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/558

0-1

1-2

2-33-44-5Page 515 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/559

0-1

1-2

2-33-44-5Page 516 of 1051

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/560

0-1

1-2

2-33-44-5Page 517 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.16.4.9	)		<u> </u>	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/561

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/562

0-1

1-2

2-33-44-5Page 519 of 1051

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/563
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 520 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.17.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/564

0-1

1-2

2-33-44-5Page 521 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/565

0-1

1-2

2-33-44-5Page 522 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/566

0-1

1-2

2-33-44-5Page 523 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.17.1.1	LO			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/567

0-1

1-2

2-33-44-5Page 524 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/568
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/569

0-1

1-2

2-33-44-5Page 525 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 526 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): 9.17.1.11								
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/570				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/571				

0-1

1-2

2-33-44-5Page 527 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/572

0-1

1-2

2-33-44-5Page 528 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.17.1.1	13	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	0-CIS-ADAP- 030524/573

0-1

1-2

2-33-44-5Page 529 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/574

0-1

1-2

2-33-44-5Page 530 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/575

0-1

1-2

2-33-44-5Page 531 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.17.1.1	15			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/576
			This vulnerability is due to incomplete error		

0-1

1-2

2-33-44-5Page 532 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/577

0-1

1-2

2-33-44-5Page 533 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/578

0-1

1-2

2-33-44-5Page 534 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.17.1.2	20			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/579

0-1

1-2

2-33-44-5Page 535 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/580

0-1

1-2

2-33-44-5Page 536 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/581

0-1

1-2

2-33-44-5Page 537 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Vers	sion(s): 9.17.1.3	30			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/582
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/583

0-1

1-2

2-33-44-5Page 538 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/584

0-1

1-2

2-33-44-5Page 539 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.17.1.3	33			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/585

0-1

1-2

**2-3** 3-4 4-5 Page **540** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/586

0-1

1-2

2-33-44-5Page 541 of 1051

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/587

0-1

1-2

2-33-44-5Page 542 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.17.1.7	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/588

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	CVE ID : CVE-2024- 20353 A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/589

0-1

1-2

2-33-44-5Page 544 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/590
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 545 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.17.1.9	)	20337		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/591

0-1

1-2

2-3 3-4 4-5 Page **546** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/592

0-1

1-2

2-33-44-5Page 547 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/593

0-1

1-2

2-3 3-4 4-5 Page **548** of **1051**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 9.18.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/594

0-1

1-2

2-3 3-4 4-5 Page **549** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/595
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/596

0-1

1-2

2-33-44-5Page 550 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 551 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): 9.18.1.3							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/597			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/598			

0-1

1-2

2-33-44-5Page 552 of 1051

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/599

0-1

1-2

2-33-44-5Page 553 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.18.2		CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/600

0-1

1-2

2-33-44-5Page 554 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/601

0-1

1-2

2-33-44-5Page 555 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/602

0-1

1-2

**2-3** 3-4 4-5 Page **556** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.18.2.5	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/603
			This vulnerability is due to incomplete error		

0-1

1-2

2-33-44-5Page 557 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/604

0-1

1-2

**2-3** 3-4 4-5 Page **558** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/605

0-1

1-2

2-33-44-5Page 559 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.18.2.7	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/606

0-1

1-2

2-33-44-5Page 560 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/607

0-1

1-2

2-33-44-5Page 561 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/608

0-1

1-2

2-33-44-5Page 562 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.18.2.8</mark>	}			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/609
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/610

0-1

1-2

2-33-44-5Page 563 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/611

0-1

1-2

2-3 3-4 4-5 Page 564 of 1051 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.18.3		<u> </u>		
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/612

0-1

1-2

2-33-44-5Page 565 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/613

0-1

1-2

2-3 3-4 4-5 Page 566 of 1051 6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/614

0-1

1-2

2-33-44-5Page 567 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.18.3.3	39		<u> </u>	<u> </u>
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/615

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	CVE ID : CVE-2024- 20353 A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/616

0-1

1-2

2-3 3-4 4-5 Page 569 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/617
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 570 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.18.3.4	6			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/618

0-1

1-2

2-33-44-5Page 571 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/619

0-1

1-2

2-33-44-5Page 572 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/620

0-1

1-2

2-33-44-5Page 573 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.18.3.5	53			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/621

0-1

1-2

2-33-44-5Page 574 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/622
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/623

0-1

1-2

2-33-44-5Page 575 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 576 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): 9.18.3.55							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/624			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/625			

0-1

1-2

2-33-44-5Page 577 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/626

0-1

1-2

2-33-44-5Page 578 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.18.3.5	56	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	0-CIS-ADAP- 030524/627

0-1

1-2

2-33-44-5Page 579 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/628

0-1

1-2

**2-3** 3-4 4-5 Page **580** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/629

0-1

1-2

2-33-44-5Page 581 of 1051

5-6

6-7

7-8

1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.18.4A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threathttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- WorkureD20-Cl 0.0-Cl 0.001111111111111111111111111111111111				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Outallow an unauthenticated, remote attacker to cause the device to reload unexpectedly,https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software unauthenticated, remote attacker to cause the device to reload unexpectedly,https://sec.cl oudapps.cisco .com/security /security https://sec.cl oudapps.cisco .com/security https://sec.cl oudapps.cisco .com/security https://sec.cl oudapps.cisco .com/security https://sec.cl oudapps.cisco .com/security https://sec.cl oudapps.cisco .com/security .com/security .com/security .com/security .com/security .com/security .com/security .com/security .com/security .com/security .com/security .com/security .com/security	Affected Ver	sion(s): 9.18.4				
service (DoS) condition. This vulnerability is	Unreachabl e Exit Condition ('Infinite	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	0-CIS-ADAP- 030524/630

0-1

1-2

2-33-44-5Page 582 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/631

0-1

1-2

2-33-44-5Page 583 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/632

0-1

1-2

**2-3** 3-4 4-5 Page **584** of **1051**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.18.4.5	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/633

0-1

1-2

2-33-44-5Page 585 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/634

0-1

1-2

**2-3** 3-4 4-5 Page **586** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/635

0-1

1-2

2-33-44-5Page 587 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.18.4.8	3			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/636
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/637

0-1

1-2

**2-3** 3-4 4-5 Page **588** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/638

0-1

1-2

**2-3** 3-4 4-5 Page **589** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.19.1				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/639

0-1

1-2

2-3 3-4 4-5 Page **590** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/640

0-1

1-2

2-33-44-5Page 591 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/641

0-1

1-2

2-33-44-5Page 592 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.19.1.1	2		L	L
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/642

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/643

0-1

1-2

**2-3** 3-4 4-5 Page **594** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/644
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 595 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.19.1.1	8			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/645

0-1

1-2

2-3 3-4 4-5 Page **596** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/646

0-1

1-2

2-33-44-5Page 597 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/647

0-1

1-2

**2-3** 3-4 4-5 Page **598** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
			20359		
Affected Ver	sion(s): 9.19.1.2	22			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/648

0-1

1-2

2-3 3-4 4-5 Page **599** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/649
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/650

0-1

1-2

**2-3** 3-4 4-5 Page **600** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 601 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): 9.19.1.24								
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/651				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/652				

0-1

1-2

2-33-44-5Page 602 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/653

0-1

1-2

2-33-44-5Page 603 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.19.1.2	27	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/654

0-1

1-2

2-33-44-5Page 604 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/655

0-1

1-2

2-33-44-5Page 605 of 1051

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/656

0-1

1-2

2-3 3-4 4-5 Page 606 of 1051 5-6

6-7

Loop with Unreachable c Exit Condition (Thrinite Loop)')24-Apr-20248.6A vulnerability is copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could aller system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359https://sec.cl oudaps.cisco o.com/security /center/conte nt/Software could allow an unauthenticated, remote attacker to cause the device to cause the device of across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359https://sec.cl oudaps.cisco o.com/security /center/conte nt/CiscoSecurity Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to crease the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudaps.cisco .com/security /center/conte nt/Advisory/ci sco-sa-asathd- websrys-dos- X8gNucD20-CIS-ADAP- 030524/657	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.19.1.5A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security 0-CIS-ADAP- 030524/657				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD20-CIS-ADAP- 030524/657						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci S030524/657O-CIS-ADAP- 030524/657	Affected Ver	sion(s): 9.19.1.5	5			
	Loop with Unreachabl e Exit Condition ('Infinite			management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	

0-1

1-2

2-33-44-5Page 607 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/658

0-1

1-2

**2-3** 3-4 4-5 Page **608** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/659

0-1

1-2

**2-3** 3-4 4-5 Page **609** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.19.1.9	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/660

0-1

1-2

2-33-44-5Page 610 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/661

0-1

1-2

2-33-44-5Page 611 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/662

0-1

1-2

2-33-44-5Page 612 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.20.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/663
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/664

0-1

1-2

2-33-44-5Page 613 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/665

0-1

1-2

2-33-44-5Page 614 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.20.1.5	5			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/666

0-1

1-2

2-33-44-5Page 615 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/667

0-1

1-2

2-33-44-5Page 616 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/668

0-1

1-2

2-33-44-5Page 617 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.20.2				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/669

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	CVE ID : CVE-2024- 20353 A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/670

0-1

1-2

2-33-44-5Page 619 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b> 2025 9		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/671
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 620 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.1				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/672

0-1

1-2

2-33-44-5Page 621 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/673

0-1

1-2

2-33-44-5Page 622 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/674

0-1

1-2

2-33-44-5Page 623 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.1.5			I	I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/675

0-1

1-2

2-33-44-5Page 624 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/676
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/677

0-1

1-2

 2-3
 3-4
 4-5

 Page 625 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 626 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): 9.8.1.7							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/678			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/679			

0-1

1-2

2-33-44-5Page 627 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/680

0-1

1-2

2-33-44-5Page 628 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.8.2		CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/681

0-1

1-2

 2-3
 3-4
 4-5

 Page 629 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/682

0-1

1-2

2-33-44-5Page 630 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/683

0-1

1-2

2-33-44-5Page 631 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.2.14	k.			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/684
			This vulnerability is due to incomplete error		

0-1

1-2

2-33-44-5Page 632 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/685

0-1

1-2

2-33-44-5Page 633 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/686

0-1

1-2

2-33-44-5Page 634 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.2.15	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/687

0-1

1-2

2-33-44-5Page 635 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/688

0-1

1-2

2-33-44-5Page 636 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/689

0-1

1-2

2-33-44-5Page 637 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.8.2.1</mark> 7	7			I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/690
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/691

0-1

1-2

2-33-44-5Page 638 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/692

0-1

1-2

2-33-44-5Page 639 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.2.20	)			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/693

0-1

1-2

**2-3** 3-4 4-5 Page **640** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/694

0-1

1-2

2-33-44-5Page 641 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/695

0-1

1-2

2-33-44-5Page 642 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	<mark>sion(s): 9.8.2.24</mark>	ŀ			<u> </u>
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/696

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/697

0-1

1-2

2-33-44-5Page 644 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/698
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 645 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver		j	20337		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/699

0-1

1-2

2-3 3-4 4-5 Page 646 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/700

0-1

1-2

2-33-44-5Page 647 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/701

0-1

1-2

**2-3** 3-4 4-5 Page **648** of **1051**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.2.28	}			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/702

0-1

1-2

2-33-44-5Page 649 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/703
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/704

0-1

1-2

2-33-44-5Page 650 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 651 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.8.2.33	3			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/705
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/706

0-1

1-2

2-33-44-5Page 652 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/707

0-1

1-2

2-33-44-5Page 653 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.8.2.35	5	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	0-CIS-ADAP- 030524/708

0-1

1-2

2-33-44-5Page 654 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/709

0-1

1-2

2-33-44-5Page 655 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/710

0-1

1-2

**2-3** 3-4 4-5 Page **656** of **1051**  5-6

6-7

Loop with Unreachable C Stition24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Adaptive Security Applance (ASA) Software and Cisco Firepower Threat Define (Tisto Security Define (Condition, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVF ID : CVF-2024- 20359https://sec.cl oudapps.cisco .orm/security /center/conte nt/CiscoSecurity Adaptive Security Applance (ASA) Software and Cisco Firepower Threat Define (CTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.https://sec.cl oudapps.cisco .orm/security .orm/security .orm/security .orm/security .orm/security .orm/security .com/sec	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.2.38A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security 0-CIS-ADAP- 030524/711				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security 0-CIS-ADAP- 030524/711						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur 030524/711	Affected Ver	sion(s): 9.8.2.38	3			
This vulnerability is	Loop with Unreachabl e Exit Condition ('Infinite			management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	

0-1

1-2

2-33-44-5Page 657 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/712

0-1

1-2

**2-3** 3-4 4-5 Page **658** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/713

0-1

1-2

2-33-44-5Page 659 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.8.2.8</mark>				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/714

0-1

1-2

2-33-44-5Page 660 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/715

0-1

1-2

2-33-44-5Page 661 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/716

0-1

1-2

2-33-44-5Page 662 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.3				I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/717
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/718

0-1

1-2

2-33-44-5Page 663 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/719

0-1

1-2

**2-3** 3-4 4-5 Page **664** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.3.11				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/720

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/721

0-1

1-2

**2-3** 3-4 4-5 Page **666** of **1051**  6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/722

0-1

1-2

2-33-44-5Page 667 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.3.14	ŀ			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/723

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/724

0-1

1-2

**2-3** 3-4 4-5 Page **669** of **1051**  6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/725
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 670 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.3.16	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/726

0-1

1-2

2-33-44-5Page 671 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/727

0-1

1-2

2-33-44-5Page 672 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/728

0-1

1-2

2-33-44-5Page 673 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.3.18	}			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/729

0-1

1-2

2-33-44-5Page 674 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/730
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/731

0-1

1-2

2-33-44-5Page 675 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 676 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): 9.8.3.21							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/732			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/733			

0-1

1-2

2-33-44-5Page 677 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/734

0-1

1-2

2-33-44-5Page 678 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.8.3.26		CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	0-CIS-ADAP- 030524/735

0-1

1-2

2-33-44-5Page 679 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/736

0-1

1-2

**2-3** 3-4 4-5 Page **680** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/737

0-1

1-2

2-33-44-5Page 681 of 1051

5-6

6-7

0-1

1-2

2-33-44-5Page 682 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/739

0-1

1-2

2-33-44-5Page 683 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/740

0-1

1-2

**2-3** 3-4 4-5 Page **684** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.8.3.8</mark>				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/741

0-1

1-2

2-33-44-5Page 685 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/742

0-1

1-2

**2-3** 3-4 4-5 Page **686** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/743

0-1

1-2

2-33-44-5Page 687 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.8.4</mark>				I
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/744
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/745

0-1

1-2

**2-3** 3-4 4-5 Page **688** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/746

0-1

1-2

**2-3** 3-4 4-5 Page **689** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.4.10	)			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ADAP- 030524/747

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/748

0-1

1-2

2-33-44-5Page 691 of 1051

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/749

0-1

1-2

2-33-44-5Page 692 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Vers	sion(s): 9.8.4.12	2			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/750

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/751

0-1

1-2

**2-3** 3-4 4-5 Page **694** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/752
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 695 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.4.15	5	20007		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/753

0-1

1-2

2-3 3-4 4-5 Page 696 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/754

0-1

1-2

2-33-44-5Page 697 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/755

0-1

1-2

**2-3** 3-4 4-5 Page **698** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.4.17	7			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/756

0-1

1-2

**2-3** 3-4 4-5 Page **699** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/757
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/758

0-1

1-2

2-33-44-5Page 700 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 701 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.8.4.20	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/759
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/760

0-1

1-2

2-33-44-5Page 702 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/761

0-1

1-2

2-33-44-5Page 703 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.8.4.22	2	CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/762

0-1

1-2

2-33-44-5Page 704 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/763

0-1

1-2

2-33-44-5Page 705 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/764

0-1

1-2

2-3 3-4 4-5 Page **706** of **1051**  5-6

6-7

1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.4.25A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security0-CIS-ADAP- 030524/765				flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD20-CIS-ADAP- 030524/765						
Loop with Unreachabl e Exit Condition ('Infinite Loop')24-Apr-20248.6management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur tityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD20-CIS-ADAP- 030524/765	Affected Ver	sion(s): 9.8.4.25	5			
This vulnerability is	Unreachabl e Exit Condition ('Infinite	24-Apr-2024	8.6	management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos-	0-CIS-ADAP- 030524/765

0-1

1-2

2-33-44-5Page 707 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/766

0-1

1-2

2-3 3-4 4-5 Page **708** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/767

0-1

1-2

2-3 3-4 4-5 Page **709** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.4.26	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/768

0-1

1-2

2-33-44-5Page 710 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/769

0-1

1-2

2-33-44-5Page 711 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/770

0-1

1-2

2-33-44-5Page 712 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.4.29	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/771
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/772

0-1

1-2

2-33-44-5Page 713 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/773

0-1

1-2

2-33-44-5Page 714 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.4.3				
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/774

0-1

1-2

2-33-44-5Page 715 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/775

0-1

1-2

2-33-44-5Page 716 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/776

0-1

1-2

2-33-44-5Page 717 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	<mark>sion(s): 9.8.4.3</mark> 2	2			<u> </u>
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/777

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/778

0-1

1-2

2-33-44-5Page 719 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/779
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 720 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.4.3	3	20337		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/780

0-1

1-2

2-33-44-5Page 721 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/781

0-1

1-2

2-33-44-5Page 722 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/782

0-1

1-2

2-33-44-5Page 723 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.4.34	ŀ			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/783

0-1

1-2

2-33-44-5Page 724 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/784
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/785

0-1

1-2

2-33-44-5Page 725 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 726 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): 9.8.4.35								
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/786				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/787				

0-1

1-2

2-33-44-5Page 727 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/788

0-1

1-2

2-33-44-5Page 728 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 9.8.4.39	)	20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/789

0-1

1-2

2-33-44-5Page 729 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/790

0-1

1-2

2-33-44-5Page 730 of 1051

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/791

0-1

1-2

2-33-44-5Page 731 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Vers	sion(s): 9.8.4.4(	)			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/792
			This vulnerability is due to incomplete error		

0-1

1-2

2-33-44-5Page 732 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b> <b>20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/793

0-1

1-2

2-33-44-5Page 733 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. CVE ID : CVE-2024- 20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/794

0-1

1-2

2-33-44-5Page 734 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
			CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.8.4.4</mark> 1	L			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/795

0-1

1-2

2-33-44-5Page 735 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/796

0-1

1-2

2-33-44-5Page 736 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/797

0-1

1-2

2-33-44-5Page 737 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	<mark>sion(s): 9.8.4.4</mark> 3	3			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/798
Improper Neutralizat ion of Special Elements	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-ADAP- 030524/799

0-1

1-2

2-3 3-4 4-5 Page **738** of **1051**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/800

0-1

1-2

2-33-44-5Page 739 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.4.44	ļ.			
Loop with Unreachabl e Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cl oudapps.cisco .com/security /center/conte	O-CIS-ADAP- 030524/801

0-1

1-2

2-3 3-4 4-5 Page **740** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/802

0-1

1-2

2-33-44-5Page 741 of 1051

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/803

0-1

1-2

2-33-44-5Page 742 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.4.45				
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/804

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition.		
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024-</b>		
			20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/805

0-1

1-2

2-3 3-4 4-5 Page **744** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024-</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	20358 A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/806
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to		

0-1

1-2

2-33-44-5Page 745 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Affected Ver	sion(s): 9.8.4.46	5			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/807

0-1

1-2

2-3 3-4 4-5 Page **746** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.		
			CVE ID : CVE-2024- 20353		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/808

0-1

1-2

2-33-44-5Page 747 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as		
			root. CVE ID : CVE-2024-		
			20358		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/809

0-1

1-2

2-3 3-4 4-5 Page **748** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. CVE ID : CVE-2024- 20359		
Affected Ver	sion(s): 9.8.4.48	}			
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	O-CIS-ADAP- 030524/810

0-1

1-2

2-3 3-4 4-5 Page **749** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	0-CIS-ADAP- 030524/811
Improper Control of Generation of Code	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	0-CIS-ADAP- 030524/812

0-1

1-2

2-3 3-4 4-5 Page **750** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.	ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		

0-1

1-2

2-33-44-5Page 751 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): 9.8.4.7								
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- websrvs-dos- X8gNucD2	0-CIS-ADAP- 030524/813				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/814				

0-1

1-2

2-33-44-5Page 752 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	O-CIS-ADAP- 030524/815

0-1

1-2

2-33-44-5Page 753 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.		
			This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.		
Affected Ver	sion(s): 9.8.4.8		CVE ID : CVE-2024- 20359		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd-	O-CIS-ADAP- 030524/816

0-1

1-2

2-33-44-5Page 754 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	websrvs-dos- X8gNucD2	
			This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. <b>CVE ID : CVE-2024- 20353</b>		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- cmd-inj- ZJV8Wysm	O-CIS-ADAP- 030524/817

0-1

1-2

2-33-44-5Page 755 of 1051

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. <b>CVE ID : CVE-2024- 20358</b>		
Improper Control of Generation of Code ('Code Injection')	24-Apr-2024	6	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-asaftd- persist-rce- FLsNXF4h	0-CIS-ADAP- 030524/818

0-1

1-2

2-3 3-4 4-5 Page **756** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. <b>CVE ID : CVE-2024- 20359</b>		
Product: ios					
Affected Ver	<mark>sion(s): 17.10.1</mark>		A vulnerability in the		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/819

0-1

1-2

2-33-44-5Page 757 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024-</b>		
Affected Ver	sion(s): 17.10.1	2	20313		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/820
Affected Ver	sion(s): 17.10.1	b			1
Buffer Copy	24-Apr-2024	7.4	A vulnerability in the OSPF version 2	https://sec.cl oudapps.cisco	0-CIS-IOS 030524/821
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page <b>758</b> of <b>1051</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			(OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024-</b>	.com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	
Affected Ver	<mark>sion(s): 17.11.1</mark>		20313		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/822

0-1

1-2

2-33-44-5Page 759 of 1051

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024-</b> <b>20313</b>		
Affected Vers	sion(s): 17.11.1	a			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/823
Affected Vers	sion(s): 17.11.9	9sw			

0-1

1-2

2-3 3-4 4-5 Page **760** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/824
Affected Ver	sion(s): 17.5.1				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/825

0-1

1-2

2-33-44-5Page 761 of 1051

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>		
Affected Ver	sion(s): 17.5.1a				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/826

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2024- 20313					
Affected Ver	Affected Version(s): 17.6.1							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/827			
Affected Ver	sion(s): 17.6.1a							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/828			

0-1

1-2

2-3 3-4 4-5 Page **763** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.		
			CVE ID : CVE-2024- 20313		
Affected Ver	sion(s): 17.6.1w	7		I	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/829

0-1

1-2

2-33-44-5Page 764 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. CVE ID : CVE-2024- 20313		
Affected Ver	<mark>sion(s): 17.6.1x</mark>				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/830
Affected Ver	sion(s): 17.6.1y				
Buffer Copy without Checking Size of Input ('Classic	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe-	0-CIS-IOS 030524/831

0-1

1-2

2-33-44-5Page 765 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	ospf-dos- dR9Sfrxp	
Affected Ver	sion(s): 17.6.1z		20313		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/832

0-1

1-2

2-3 3-4 4-5 Page **766** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause the affected device to reload, resulting in a DoS condition.		
			CVE ID : CVE-2024- 20313		
Affected Ver	sion(s): 17.6.1z	1			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/833
Affected Ver	sion(s): 17.6.2				
Buffer Copy without Checking Size of Input	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci	0-CIS-IOS 030524/834

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	sco-sa-iosxe- ospf-dos- dR9Sfrxp	
Affected Ver	sion(s): 17.6.3				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/835

0-1

1-2

2-3 3-4 4-5 Page **768** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.		
			CVE ID : CVE-2024- 20313		
Affected Ver	sion(s): 17.6.3a				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/836
Affected Ver	sion(s): 17.6.4				I
Buffer Copy without Checking	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-IOS 030524/837

0-1

1-2

2-3 3-4 4-5 Page **769** of **1051**  6-7 7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	
			CVE ID : CVE-2024- 20313		
Affected Ver	sion(s): 17.6.5				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/838

0-1

1-2

2-33-44-5Page 770 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024-</b>		
			20313		
Affected Vers	sion(s): 17.6.5a			ſ	1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/839
Affected Vers	sion(s): 17.7.1				
Buffer Copy	24-Apr-2024	7.4	A vulnerability in the OSPF version 2	https://sec.cl oudapps.cisco	0-CIS-IOS 030524/840
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 771 of 1051	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			(OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	.com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	
Affected Ver	sion(s): 17.7.1a				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/841

0-1

1-2

2-33-44-5Page 772 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024-</b> <b>20313</b>					
Affected Ver	sion(s): 17.7.1b		I					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/842			
Affected Ver	sion(s): 17.7.2		<u> </u>					
	Affected Version(s): 17.7.2							

0-1

1-2

2-33-44-5Page 773 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/843
Affected Ver	sion(s): 17.8.1				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/844

0-1

1-2

2-33-44-5Page 774 of 1051

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>		
Affected Ver	sion(s): 17.8.1a				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/845

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 20313		
Affected Ver	sion(s): 17.9.1				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/846
Affected Ver	sion(s): 17.9.1a				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/847

0-1

1-2

2-3 3-4 4-5 Page **776** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.		
			CVE ID : CVE-2024- 20313		
Affected Ver	sion(s): 17.9.1w	7			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/848

0-1

1-2

2-33-44-5Page 777 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. CVE ID : CVE-2024- 20313		
Affected Ver	<mark>sion(s): 17.9.1x</mark>				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/849
Affected Ver	sion(s): 17.9.1x	1			
Buffer Copy without Checking Size of Input ('Classic	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe-	0-CIS-IOS 030524/850

0-1

1-2

2-33-44-5Page 778 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	ospf-dos- dR9Sfrxp	
Affected Ver	sion(c), 170 1		CVE ID : CVE-2024- 20313		
Allected ver	sion(s): 17.9.1y		A vulnerability in the OSPF version 2		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	(OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/851

0-1

1-2

2-33-44-5Page 779 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause the affected device to reload, resulting in a DoS condition.		
			CVE ID : CVE-2024- 20313		
Affected Ver	sion(s): 17.9.1y	1	·		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/852
Affected Ver	sion(s): 17.9.2				
Buffer Copy without Checking Size of Input	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci	0-CIS-IOS 030524/853

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	sco-sa-iosxe- ospf-dos- dR9Sfrxp	
Affected Ver	sion(s): 17.9.2a				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	O-CIS-IOS 030524/854

0-1

1-2

2-33-44-5Page 781 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.				
			CVE ID : CVE-2024- 20313				
Affected Ver	sion(s): 17.9.3						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	0-CIS-IOS 030524/855		
Affected Version(s): 17.9.3a							
Buffer Copy without Checking	24-Apr-2024	7.4	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-IOS 030524/856		

0-1

1-2

3-4 4-5 2-3 Page **782** of **1051** 

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. <b>CVE ID : CVE-2024- 20313</b>	nt/CiscoSecur ityAdvisory/ci sco-sa-iosxe- ospf-dos- dR9Sfrxp	
Vendor: Lin	ux				
Product: lin	ux_kernel				
Affected Ver	sion(s): * Up to	(excluding	g) 4.19.311		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix stackmap overflow check on 32- bit arches The stackmap code relies on roundup_pow_of_two() to compute the number	https://git.ke rnel.org/stabl e/c/0971126 c8164abe200 4b8536b4969 0a0d6005b0a, https://git.ke rnel.org/stabl e/c/1564100 7df0f0d35fa2 8742b25c2a7 db9dcd6895, https://git.ke rnel.org/stabl e/c/21e5fa46	O-LIN-LINU- 030524/857

0-1

1-2

2-33-44-5Page 783 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of hash buckets, and contains an overflow check by checking if the	88e1a4d3db6 b72216231b2 4232f75c1d	
			resulting value is 0. However, on 32-bit arches, the roundup code itself		
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code.		
			The commit in the fixes tag actually attempted to fix this, but the fix		
			did not account for the UB, so the fix only works on CPUs where an		
			overflow does result in a neat truncation to zero, which is not		
			guaranteed. Checking the value before rounding does not have this		
			problem.		
			CVE ID : CVE-2024- 26883		

0-1

1-2

**2-3** 3-4 4-5 Page **784** of **1051**  5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		In the Linux kernel, the following vulnerability has been resolved:			
			Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security		
NULL Pointer Dereferenc e	ter 17-Apr-2024 55	7-Apr-2024 5.5	During our fuzz testing of the connection and disconnection process at the RFCOMM layer, we discovered this bug. By comparing the packets from a normal connection and disconnection process with the testcase that triggered a KASAN report. We analyzed the cause of this bug as follows:	097e82407dd 030524/85 429a202cde9 a73d3ae29b, https://git.ke rnel.org/stabl e/c/3ead59ba fad05f2967ae 2438c0528d5 3244cfde5	0-LIN-LINU- 030524/858
			1. In the packets captured during a normal connection, the host sends a		
			`Read Encryption Key Size` type of `HCI_CMD` packet		
			(Command Opcode: 0x1408) to the controller to inquire the length of		
			encryption key.After receiving this packet, the controller immediately		

0-1

1-2

2-33-44-5Page 785 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replies with a Command Completepacket (Event Code: 0x0e) to return the		
			Encryption Key Size.		
			2. In our fuzz test case, the timing of the controller's response to this		
			packet was delayed to an unexpected point: after the RFCOMM and L2CAP		
			layers had disconnected but before the HCI layer had disconnected.		
			3. After receiving the Encryption Key Size Response at the time described		
			in point 2, the host still called the rfcomm_check_security function.		
			However, by this time `struct l2cap_conn *conn = l2cap_pi(sk)- >chan->conn;`		
			had already been released, and when the function executed		
			`return hci_conn_security(conn ->hcon, d->sec_level, auth_type, d->out);`,		
			specifically when accessing `conn->hcon`,		

0-1

1-2

2-3 3-4 4-5 Page **786** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a null-ptr-deref error occurred.		
			To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling		
			rfcomm_recv_frame in rfcomm_process_rx.		
			CVE ID : CVE-2024- 26903		
Affected Ver	sion(s): * Up to	(excluding	g) 5.10.214	I	I
			In the Linux kernel, the following vulnerability has been resolved:		
			RDMA/mlx5: Fix fortify source warning while accessing Eth segment	https://git.ke rnel.org/stabl e/c/185fa070	
			[ cut here ]  memcpy: detected	00e0a81d54cf 8c05414cebff 14469a5c, https://git.ke	
N/A 17-A	17-Apr-2024	7.8	field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131 (size 2)	rnel.org/stabl e/c/4d5e86a 56615cc387d 21c629f9af8f b0e958d350, https://git.ke rnel.org/stabl e/c/60ba938 a8bc8c90e72 4c75f98e932f	O-LIN-LINU- 030524/859
			WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131	9fb7ae1b9d	

0-1

1-2

2-33-44-5Page 787 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mlx5_ib_post_send+0x1		
			91b/0x1a60 [mlx5_ib]		
			Modules linked in:		
			8021q garp mrp stp llc		
			rdma_ucm(OE)		
			rdma_cm(OE)		
			iw_cm(OE) ib_ipoib(OE)		
			ib_cm(OE) ib_umad(OE)		
			mlx5_ib(OE)		
			ib_uverbs(OE)		
			ib_core(OE)		
			mlx5_core(OE)		
			pci_hyperv_intf		
			mlxdevm(OE)		
			mlx_compat(OE) tls		
			mlxfw(OE) psample		
			nft_fib_inet nft_fib_ipv4		
			nft_fib_ipv6 nft_fib nft_reject_inet		
			nf_reject_ipv4		
			nf_reject_ipv6 nft_reject		
			nft_ct nft_chain_nat		
			nf_nat nf_conntrack		
			nf_defrag_ipv6		
			nf_defrag_ipv4 ip_set		
			nf_tables libcrc32c		
			nfnetlink		
			mst_pciconf(OE)		
			knem(OE) vfio_pci		
			vfio_pci_core		
			vfio_iommu_type1 vfio		
			iommufd irqbypass		
			cuse nfsv3 nfs fscache		
			netfs xfrm_user		
			xfrm_algo ipmi_devintf		
			ipmi_msghandler binfmt_misc		
			crct10dif_pclmul		
			crc32_pclmul		
			polyval_clmulni		
			polyval_generic		
			sha512_ssse3 snd_pcsp		
			aesni_intel crypto_simd		

0-1

1-2

2-3 3-4 4-5 Page **788** of **1051**  7-8

6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cryptd snd_pcm snd_timer joydev snd soundcore input_leds serio_raw evbug nfsd auth_rpcgss nfs_acl lockd grace sch_fq_codel sunrpc drm efi_pstore ip_tables x_tables autofs4 psmouse virtio_net net_failover failover floppy		
			[last unloaded: mlx_compat(OE)]		
			CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2.0-32-generic #32~22.04.1-Ubuntu		
			Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011		
			RIP: 0010:mlx5_ib_post_sen d+0x191b/0x1a60 [mlx5_ib]		
			Code: 0c 01 00 a8 01 75 25 48 8b 75 a0 b9 02 00 00 00 48 c7 c2 10 5b fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01 e8 95 4d 93 da <0f> 0b 44 8b 4d b0 4c 8b 45 c8 48 8b 4d c0 e9 49 fb ff ff 41 0f b7		
			RSP: 0018:ffffb5b48478b570 EFLAGS: 00010046		
			RAX: 00000000000000000 RBX: 000000000000000001		

0-1

1-2

2-3 3-4 4-5 Page **789** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RCX: 0000000000000000000000		
			RDX: 00000000000000000000000		
			RSI: 0000000000000000000000		
			RDI: 000000000000000000000		
			RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000		
			R10: 0000000000000000000 R11: 0000000000		
			R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80		
			FS: 00007fc03b444c80(00 00) GS:ffff963a3dc00000(0 000) knlGS:0000000000000 000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			CR2: 0000556f46bdf000 CR3: 000000006ac6003 CR4: 0000000003706f0		
			DR0: 0000000000000000 DR1: 000000000000000000000000000000000000		

0-1

1-2

2-3 3-4 4-5 Page **790** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DR2: 0000000000000000 DR3: 00000000000000000000000		
			DR6: 00000000fffe0ff0 DR7: 0000000000000400		
			Call Trace:		
			<task></task>		
			? show_regs+0x72/0x90		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?_warn+0x8d/0x160		
			? mlx5_ib_post_send+0x1		
			91b/0x1a60 [mlx5_ib]		
			?		
			report_bug+0x1bb/0x1 d0		
			?		
			handle_bug+0x46/0x90 ?		
			exc_invalid_op+0x19/0 x80		
			?		
			asm_exc_invalid_op+0x 1b/0x20		
			? 		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			mlx5_ib_post_send_nod rain+0xb/0x20 [mlx5_ib]		
			ipoib_send+0x2ec/0x77 0 [ib_ipoib]		

0-1

1-2

2-33-44-5Page 791 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ipoib_start_xmit+0x5a0 /0x770 [ib_ipoib]		
			dev_hard_start_xmit+0x 8e/0x1e0 ?		
			validate_xmit_skb_list+ 0x4d/0x80		
			sch_direct_xmit+0x116 /0x3a0		
			dev_xmit_skb+0x1fd/ 0x580		
			dev_queue_xmit+0x28 4/0x6b0 ?		
			_raw_spin_unlock_irq+0 xe/0x50 2		
			flush_work.isra.0+0x2 0d/0x370		
			? push_pseudo_header+0 x17/0x40 [ib_ipoib]		
			neigh_connected_outpu t+0xcd/0x110		
			ip_finish_output2+0x17 9/0x480 ?		
			: smp_call_single_queue +0x61/0xa0		
			ip_finish_output+0xc3 /0x190		

0-1

1-2

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_finish_output+0x2e/ 0xf0		
			ip_output+0x78/0x110 ? pfx_ip_finish_output+ 0x10/0x10		
			ip_local_out+0x64/0x7 0		
			ip_queue_xmit+0x18a /0x460		
			ip_queue_xmit+0x15/0 x30		
			tcp_transmit_skb+0x9 14/0x9c0		
			tcp_write_xmit+0x334/ 0x8d0		
			tcp_push_one+0x3c/0x 60		
			tcp_sendmsg_locked+0x 2e1/0xac0		
			tcp_sendmsg+0x2d/0x5 0		
			inet_sendmsg+0x43/0x 90		
			sock_sendmsg+0x68/0x 80		

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sock_write_iter+0x93/0 x100		
			vfs_write+0x326/0x3c0 ksys_write+0xbd/0xf0 ? do_syscall_64+0x69/0x 90 x64_sys_write+0x19/ 0x30 do_syscall_ truncated <b>CVE ID : CVE-2024-</b>		
			26907		
Affected Ver	sion(s): * Up to	(excluding	g) 5.15.71		
Improper Restriction of Operations within the Bounds of a Memory Buffer	28-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Harden accesses to the reset domains Accessing reset domains descriptors by the index upon the SCMI drivers requests through the SCMI reset operations interface can potentially lead to out-of-bound violations if the SCMI driver misbehave.	https://git.ke rnel.org/stabl e/c/1f08a1b2 6cfc53b7715a bc46857c602 3bb1b87de, https://git.ke rnel.org/stabl e/c/8e65edf0 d37698f7a6c b174608d3ec 7976baf49e, https://git.ke rnel.org/stabl e/c/e9076ffb caed5da6c18 2b144ef9f6e2 4554af268	0-LIN-LINU- 030524/860

0-1

1-2

5-6

Weakness	Publish Date         CVSSv3         Description & CVE ID		Patch	NCIIPC ID	
			Add an internal consistency check before any such domains descriptors		
			accesses.		
			CVE ID : CVE-2022- 48655		
Affected Vers	sion(s): * Up to	(excluding	g) 5.4.269		
			In the Linux kernel, the following vulnerability has been resolved:		
			netfilter: ipset: fix performance regression in swap operation	https://git.ke	
Concurrent Execution			The patch "netfilter: ipset: fix race condition between swap/destroy	rnel.org/stabl e/c/653bc5e6 d9995d7d5f4 97c665b3218	
using Shared Resource with	17-Apr-2024	4.7	and kernel side add/del/test", commit 28628fa9 fixes a race condition.	75a626161c, https://git.ke rnel.org/stabl e/c/970709a	O-LIN-LINU-
Improper Synchroniz ation ('Race Condition')	I		But the synchronize_rcu() added to the swap function unnecessarily slows	67696b100a5 7b33af1a3d7 5fc34b747eb, https://git.ke rnel.org/stabl	030524/861
,			it down: it can safely be moved to destroy and use call_rcu() instead.	e/c/97f7cf1cd 80eeed3b7c8 08b7c124632 95c751001	
			Eric Dumazet pointed out that simply calling the destroy functions as		
			rcu callback does not work: sets with timeout use garbage collectors		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which need cancelling at destroy which can wait. Therefore the destroy		
			functions are split into two: cancelling garbage collectors safely at		
			executing the command received by netlink and moving the remaining		
			part only into the rcu callback.		
			CVE ID : CVE-2024- 26910		
Affected Ver	sion(s): * Up to	(excluding	g) 5.4.273		
			In the Linux kernel, the following vulnerability has been resolved:		
			btrfs: fix data race at btrfs_use_block_rsv() when accessing block reserve	https://git.ke rnel.org/stabl e/c/2daa2a8e 895e6dc2395 f8628c011bcf 1e019040d,	
Improper	17 4 2024		At btrfs_use_block_rsv() we read the size of a block reserve without	https://git.ke rnel.org/stabl e/c/7e9422d	O-LIN-LINU-
Locking	17-Apr-2024	r-2024 5.5	locking its spinlock, which makes KCSAN complain because the size of a	35d574b6462 69ca46010a8 35ca074b310, https://git.ke rnel.org/stabl	030524/862
			block reserve is always updated while holding its spinlock. The report from KCSAN is the	e/c/ab1be3f1 aa7799f9915 5488c28eacae f65eb68fb	
			following: [653.313148] BUG:		
			KCSAN: data-race in		

0-1

1-2

2-3 3-4 4-5 Page **796** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			btrfs_update_delayed_r efs_rsv [btrfs] / btrfs_use_block_rsv [btrfs]		
			[653.314755] read to 0x000000017f5871b8 of 8 bytes by task 7519 on cpu 0:		
			[653.314779] btrfs_use_block_rsv+0x e4/0x2f8 [btrfs]		
			[653.315606] btrfs_alloc_tree_block+0 xdc/0x998 [btrfs]		
			[653.316421] btrfs_force_cow_block+ 0x220/0xe38 [btrfs]		
			[653.317242] btrfs_cow_block+0x1ac /0x568 [btrfs]		
			[653.318060] btrfs_search_slot+0xda 2/0x19b8 [btrfs]		
			[653.318879] btrfs_del_csums+0x1dc /0x798 [btrfs]		
			[653.319702] btrfs_free_extent.isra. 0+0xc24/0x2028 [btrfs]		
			[653.320538] btrfs_run_delayed_ref s+0xd3c/0x2390 [btrfs]		
			[653.321340] btrfs_run_delayed_refs+ 0xae/0x290 [btrfs]		
			[653.322140] flush_space+0x5e4/0x7 18 [btrfs]		

0-1

1-2

2-33-44-5Page 797 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.322958] btrfs_preempt_reclaim_ metadata_space+0x102 /0x2f8 [btrfs]		
			[653.323781] process_one_work+0x3 b6/0x838		
			[653.323800] worker_thread+0x75e/ 0xb10		
			[653.323817] kthread+0x21a/0x230		
			[653.323836] ret_from_fork+0x6c/0 xb8		
			[653.323855] ret_from_fork+0xa/0x3 0		
			[653.323887] write to 0x000000017f5871b8 of 8 bytes by task 576 on cpu 3:		
			[653.323906] btrfs_update_delayed_r efs_rsv+0x1a4/0x250 [btrfs]		
			[653.324699] btrfs_add_delayed_data _ref+0x468/0x6d8 [btrfs]		
			[653.325494] btrfs_free_extent+0x76 /0x120 [btrfs]		
			[653.326280] btrfs_mod_ref+0x6a8/ 0x6b8 [btrfs]		
			[653.327064] btrfs_dec_ref+0x50/0x7 0 [btrfs]		

0-1

1-2

2-3 3-4 4-5 Page **798** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.327849] walk_up_proc+0x236/0 xa50 [btrfs]		
			[653.328633] walk_up_tree+0x21c/0x 448 [btrfs]		
			[653.329418] btrfs_drop_snapshot+0x 802/0x1328 [btrfs]		
			[653.330205] btrfs_clean_one_deleted _snapshot+0x184/0x23 8 [btrfs]		
			[653.330995] cleaner_kthread+0x2b0 /0x2f0 [btrfs]		
			[653.331781] kthread+0x21a/0x230		
			[653.331800] ret_from_fork+0x6c/0 xb8		
			[653.331818] ret_from_fork+0xa/0x3 0		
			So add a helper to get the size of a block reserve while holding the lock.		
			Reading the field while holding the lock instead of using the data_race()		
			annotation is used in order to prevent load tearing.		
			CVE ID : CVE-2024- 26904		
Affected Ver	sion(s): * Up to	(excludin	g) 6.6.23		

0-1

1-2

2-3 3-4 4-5 Page **799** of **1051**  6-7 7-8

5-6

Weakness	Publish Date         CVSSv3         Description & CVE ID		Description & CVE ID	Patch	NCIIPC ID
Weakness NULL Pointer Dereferenc e	Publish Date	<b>CVSSv3</b>	Description & CVE ID In the Linux kernel, the following vulnerability has been resolved: perf: RISCV: Fix panic on pmu overflow handler (1 << idx) of int is not desired when setting bits in unsigned long overflowed_ctrs, use BIT() instead. This panic happens when running 'perf record -e branches' on sophgo sg2042. [ 273.311852] Unable to handle kernel NULL pointer dereference at virtual address 00000000000098 [ 273.320851] Oops [#1] [ 273.323179] Modules linked in: [ 273.326303] CPU: 0 PID: 1475 Comm: perf Not tainted 6.6.0-rc3+ #9	Patch https://git.ke rnel.org/stabl e/c/34b5678 68777e9fd39 ec533396972 8a7f0cf179c, https://git.ke rnel.org/stabl e/c/3ede8e94 de6b834b48b 0643385e663 63e7a04be9, https://git.ke rnel.org/stabl e/c/9f599ba3 b9cc4bdb8ec 1e3f0feddd41 bf9d296d6	NCIIPC ID
			PID: 1475 Comm: perf Not tainted 6.6.0-rc3+		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 273.342291] ra : pmu_sbi_ovf_handler+0 x2e0/0x34e		
			[ 273.347091] epc : ffffffff80aecd98 ra : ffffffff80aee056 sp : ffffffff6e36928b0		
			[ 273.354454] gp : fffffff821f82d0 tp : ffffffd90c353200 t0 : 0000002ade4f9978		
			[ 273.361815] t1 : 0000000000504d55 t2 : fffffff8016cd8c s0 : fffffff6e3692a70		
			[ 273.369180] s1: 0000000000000020 a0 : 0000000000000000 a1: 00001a8e81800000		
			[ 273.376540] a2 : 0000003c00070198 a3 : 0000003c00db75a4 a4 : 00000000000000015		
			[ 273.383901] a5 : ffffffd7ff8804b0 a6 : 0000000000000015 a7 : 000000000000002a		
			[ 273.391327] s2 : 0000000000000ffff s3 : 00000000000000000 s4 : fffffd7ff8803b0		
			[ 273.398773] s5 : 0000000000504d55 s6 : ffffffd905069800 s7 : ffffffff821fe210		
			[ 273.406139] s8 : 000000007fffffff s9 : ffffffd7ff8803b0 s10: ffffffd903f29098		

0-1

1-2

2-33-44-5Page 801 of 1051

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 273.413660] s11: 0000000080000000 t3 : 0000000000000003 t4 : fffffff8017a0ca		
			[ 273.421022] t5 : ffffffff8023cfc2 t6 : ffffffd9040780e8		
			[ 273.426437] status: 0000000200000100 badaddr: 0000000000000098		
			cause: 000000000000000000d		
			[ 273.434512] [ <ffffffff80aecd98>] riscv_pmu_ctr_get_widt h_mask+0x8/0x62</ffffffff80aecd98>		
			[ 273.441169] [ <ffffffff80076bd8>] handle_percpu_devid_ir q+0x98/0x1ee</ffffffff80076bd8>		
			[ 273.447562] [ <ffffffff80071158>] generic_handle_domain _irq+0x28/0x36</ffffffff80071158>		
			[ 273.454151] [ <ffffffff8047a99a>] riscv_intc_irq+0x36/0x 4e</ffffffff8047a99a>		
			[ 273.459659] [ <ffffffff80c944de>] handle_riscv_irq+0x4a/ 0x74</ffffffff80c944de>		
			[ 273.465442] [ <ffffffff80c94c48>] do_irq+0x62/0x92</ffffffff80c94c48>		
			[ 273.470360] Code: 0420 60a2 6402 5529 0141 8082 0013 0000 0013 0000 (6d5c) b783		

0-1

1-2

2-33-44-5Page 802 of 1051

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Descrip	tion & CVI	ID	Pate	ch	NCI	IPC ID
			trace 00000000 - [ 273.482 panic - no Fatal exce interrupt	00000000000000000000000000000000000000					
Affected Ver	sion(s): * Up to	(excludin	g) 6.7.6						
Integer Underflow (Wrap or Wraparoun d)	17-Apr-2024	7.8	g) 6.7.6 In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix dcn35 8k30 Underflow/Corruption Issue [why] odm calculation is missing for pipe split policy determination and cause Underflow/Corruption issue. [how] Add the odm calculation. <b>CVE ID : CVE-2024- 26913</b>		https:// rnel.org e/c/cdb 874c631 b8c38e5 cbdd186 https:// rnel.org e/c/faf5 1bc42a6 9457323 20c7076	/stabl e0be8 oca85 5b1ee df31, git.ke /stabl 1b20 df500 abb62		-LINU- 24/864	
Affected Ver	sion(s): From (e	excluding	5.15 Up to	(excludi	ng) 5.1	5.71			
N/A	28-Apr-2024	7.8	following vulnerability has been resolved: 48b				git.ke /stabl 03b2 3eb49 e5d33		-LINU- 24/865
CVSS Scoring S	Scale 0-1	1-2 2	2- <b>3</b> 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm: slub: fix flush_cpu_slab()/_free_ slab() invocations in task context.	18e6d8f3c5b, https://git.ke rnel.org/stabl e/c/df6cb393 35cf5a1b918e	
			Commit 5a836bf6b09f ("mm: slub: move flush_cpu_slab() invocations free_slab() invocations out of IRQ context") moved all flush_cpu_slab() invocations to the global workqueue to avoid a problem related with deactivate_slab()/free _slab() being called from an IRQ context on PREEMPT_RT kernels.	8dbd8ba7cd9 f1d00e45a, https://git.ke rnel.org/stabl e/c/e45cc288 724f0cfd497b b5920bcfa60c aa335729	
			When the flush_all_cpu_locked() function is called from a task context it may happen that a workqueue with WQ_MEM_RECLAIM bit set ends up flushing the global workqueue, this will cause a dependency issue.		
			workqueue: WQ_MEM_RECLAIM nvme-delete-		

0-1

1-2

2-3 3-4 4-5 Page 804 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wq:nvme_delete_ctrl_w ork [nvme_core]		
			is flushing !WQ_MEM_RECLAIM events:flush_cpu_slab		
			WARNING: CPU: 37 PID: 410 at kernel/workqueue.c:26 37		
			check_flush_dependenc y+0x10a/0x120		
			Workqueue: nvme- delete-wq nvme_delete_ctrl_work [nvme_core]		
			RIP: 0010:check_flush_depe ndency+0x10a/0x120[ 453.262125] Call Trace:		
			flush_work.isra.0+0xb f/0x220		
			? queue_work+0x1dc/0 x420		
			flush_all_cpus_locked+0 xfb/0x120		
			kmem_cache_shutdow n+0x2b/0x320		
			kmem_cache_destroy+0 x49/0x100		
			bioset_exit+0x143/0x1 90		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			blk_release_queue+0xb 9/0x100			
			kobject_cleanup+0x37/ 0x130			
			nvme_fc_ctrl_free+0xc6 /0x150 [nvme_fc]			
			nvme_free_ctrl+0x1ac/ 0x2b0 [nvme_core]			
			Fix this bug by creating a workqueue for the flush operation with			
			the WQ_MEM_RECLAIM bit set.			
			CVE ID : CVE-2022- 48658			
Affected Ver	sion(s): From (e	excluding)	5.16 Up to (excluding) 5.1	9.12		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/1f08a1b2 6cfc53b7715a bc46857c602		
Improper Restriction of Operations	28-Apr-2024	7.8	firmware: arm_scmi: Harden accesses to the reset domains	3bb1b87de, https://git.ke rnel.org/stabl e/c/8e65edf0	O-LIN-LINU-	
within the Bounds of a Memory Buffer	20-Api-2024 7.	7.8	7.0	Accessing reset domains descriptors by the index upon the SCMI drivers	d37698f7a6c b174608d3ec 7976baf49e, https://git.ke	030524/866
			requests through the SCMI reset operations interface can	rnel.org/stabl e/c/e9076ffb caed5da6c18 2b144ef9f6e2		
			potentially	4554af268		

0-1

1-2

**2-3** 3-4 4-5 Page **806** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to out-of-bound violations if the SCMI driver misbehave.		
			Add an internal consistency check before any such domains descriptors accesses.		
			CVE ID : CVE-2022- 48655		
N/A	28-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: mm: slub: fix flush_cpu_slab()/_free_ slab() invocations in task context. Commit 5a836bf6b09f ("mm: slub: move flush_cpu_slab() invocations free_slab() invocations out of IRQ context") moved all flush_cpu_slab() invocations to the global workqueue to avoid a problem related with deactivate_slab()/free slab() being called from an IRQ context on PREEMPT_RT kernels.	https://git.ke rnel.org/stabl e/c/61703b2 48be993eb49 97b00ae5d33 18e6d8f3c5b, https://git.ke rnel.org/stabl e/c/df6cb393 35cf5a1b918e 8dbd8ba7cd9 f1d00e45a, https://git.ke rnel.org/stabl e/c/e45cc288 724f0cfd497b b5920bcfa60c aa335729	0-LIN-LINU- 030524/867

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When the flush_all_cpu_locked() function is called from a task context		
			it may happen that a workqueue with WQ_MEM_RECLAIM bit set ends up		
			flushing the global workqueue, this will cause a dependency issue.		
			workqueue: WQ_MEM_RECLAIM nvme-delete- wq:nvme_delete_ctrl_w ork [nvme_core]		
			is flushing !WQ_MEM_RECLAIM events:flush_cpu_slab		
			WARNING: CPU: 37 PID: 410 at kernel/workqueue.c:26 37		
			check_flush_dependenc y+0x10a/0x120		
			Workqueue: nvme- delete-wq nvme_delete_ctrl_work [nvme_core]		
			RIP: 0010:check_flush_depe ndency+0x10a/0x120[ 453.262125] Call Trace:		
			flush_work.isra.0+0xb f/0x220		

0-1

1-2

**2-3** 3-4 4-5 Page **808** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? queue_work+0x1dc/0 x420		
			flush_all_cpus_locked+0 xfb/0x120		
			kmem_cache_shutdow n+0x2b/0x320		
			kmem_cache_destroy+0 x49/0x100		
			bioset_exit+0x143/0x1 90		
			blk_release_queue+0xb 9/0x100		
			kobject_cleanup+0x37/ 0x130		
			nvme_fc_ctrl_free+0xc6 /0x150 [nvme_fc]		
			nvme_free_ctrl+0x1ac/ 0x2b0 [nvme_core]		
			Fix this bug by creating a workqueue for the flush operation with		
			the WQ_MEM_RECLAIM bit set.		
			CVE ID : CVE-2022- 48658		
Affected Ver	sion(s): From (e	excluding)	6.7.0 Up to (excluding) 6.7	7.6	
Missing Release of Memory	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/042b5f83	O-LIN-LINU- 030524/868

 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
after Effective Lifetime			drm/nouveau: fix several DMA buffer leaks	841fbf7ce394 74412db3b5e 4765a7ea7, https://git.ke rnel.org/stabl	
			Nouveau manages GSP- RM DMA buffers with nvkm_gsp_mem objects. Several of	e/c/6190d4c 08897d748dd 25f0b78267a 90aa1694e15	
			these buffers are never dealloced. Some of them can be deallocated		
			right after GSP-RM is initialized, but the rest need to stay until the		
			driver unloads.		
			Also futher bullet-proof these objects by poisoning the buffer and		
			clearing the nvkm_gsp_mem object when it is deallocated. Poisoning		
			the buffer should trigger an error (or crash) from GSP-RM if it tries		
			to access the buffer after we've deallocated it, because we were wrong		
			about when it is safe to deallocate.		
			Finally, change the mem->size field to a		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			size_t because that's the same type that dma_alloc_coherent expects. CVE ID : CVE-2024- 26912		
Improper Handling of Exceptiona l Conditions	17-Apr-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: drm/buddy: Fix alloc_range() error handling code Few users have observed display corruption when they boot the machine to KDE Plasma or playing games. We have root caused the problem that whenever alloc_range() couldn't find the required memory blocks the function was returning SUCCESS in some of the corner cases. The right approach would be if the total allocated size is less than the required size, the function should return -ENOSPC.	https://git.ke rnel.org/stabl e/c/4b59c3fa da06e5e8010 ef7700689c7 1986e667a2, https://git.ke rnel.org/stabl e/c/8746c6c9 dfa31d269c6 5dd52ab42fd e0720b7d91	0-LIN-LINU- 030524/869

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2024- 26911				
Affected Version(s): From (including) 2.6.22 Up to (excluding) 4.19.311							
			In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem in aoecmd cfg pkts				
Use After Free	17-Apr-2024	7.8	in aoecmd_cfg_pkts This patch is against CVE-2023-6270. The description of cve is: A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on `struct net_device`, and a use-after-free can be triggered by racing between the free on the struct and the access through the `skbtxq` global queue. This could lead to a denial of service condition or	https://git.ke rnel.org/stabl e/c/079cba4f 4e307c69878 226fdf5228c2 0aa1c969c, https://git.ke rnel.org/stabl e/c/1a54aa50 6b3b2f31496 731039e4977 8f54eee881, https://git.ke rnel.org/stabl e/c/74ca3ef6 8d2f449bc84 8c0a814cefc4 87bf755fa	O-LIN-LINU- 030524/870		
			potential code execution. In aoecmd_cfg_pkts(), it always calls				

0-1

1-2

2-33-44-5Page 812 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dev_put(ifp) when skb initial		
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		
			This patch removed the dev_put(ifp) in the success path in		
			aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx().		
			CVE ID : CVE-2024- 26898		
Affected Ver	sion(s): From (i	ncluding)	2.6.22 Up to (excluding) 4	.9.330	
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/016b150 992eebc32c4	
N/A	28-Apr-2024	5.5	mm/slub: fix to return errno if kmalloc() fails	a18f783cf2bb 6e2545a3d9, https://git.ke rnel.org/stabl	O-LIN-LINU- 030524/871
			In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to	e/c/02bcd95 1aa3c2cea95f b241c20802e 9501940296,	

0-1

1-2

2-33-44-5Page 813 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-memory, if it fails, return errno correctly rather than triggering panic via BUG_ON();	https://git.ke rnel.org/stabl e/c/2d6e55e 0c03804e1e2 27b80a5746e 086d6c6696c	
			kernel BUG at mm/slub.c:5893! Internal error: Oops - BUG: 0 [#1] PREEMPT SMP		
			Call trace: sysfs_slab_add+0x258/		
			0x260 mm/slub.c:5973 kmem_cache_create+ 0x60/0x118 mm/slub.c:4899 create_cache mm/slab_common.c:22 9 [inline]		
			kmem_cache_create_use rcopy+0x19c/0x31c mm/slab_common.c:33 5		
			kmem_cache_create+0x 1c/0x28 mm/slab_common.c:39 0		
			f2fs_kmem_cache_creat e fs/f2fs/f2fs.h:2766 [inline]		
			f2fs_init_xattr_caches+0		

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x78/0xb4 fs/f2fs/xattr.c:808		
			f2fs_fill_super+0x1050/ 0x1e0c fs/f2fs/super.c:4149		
			mount_bdev+0x1b8/0x 210 fs/super.c:1400 f2fs_mount+0x44/0x58		
			fs/f2fs/super.c:4512 legacy_get_tree+0x30/0 x74 fs/fs_context.c:610		
			vfs_get_tree+0x40/0x1 40 fs/super.c:1530		
			do_new_mount+0x1dc/ 0x4e4 fs/namespace.c:3040		
			path_mount+0x358/0x 914 fs/namespace.c:3370		
			do_mount fs/namespace.c:3383 [inline]		
			do_sys_mount fs/namespace.c:3591 [inline]		
			se_sys_mount fs/namespace.c:3568 [inline]		
			arm64_sys_mount+0x 2f8/0x408 fs/namespace.c:3568		
			CVE ID : CVE-2022- 48659		

0-1

1-2

2-33-44-5Page 815 of 1051

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	2.6.39 Up to (excluding) 4	.19.311	
Use of Uninitialize d Resource	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak syzbot identified a kernel information leak vulnerability in do_sys_name_to_handle () and issued the following report [1]. [1] "BUG: KMSAN: kernel- infoleak in instrument_copy_to_use r include/linux/instrume nted.h:114 [inline] BUG: KMSAN: kernel- infoleak in _copy_to_user+0xbc/0x 100 lib/usercopy.c:40 instrument_copy_to_use r include/linux/instrume nted.h:114 [inline] _copy_to_user+0xbc/0x 100 lib/usercopy.c:40	https://git.ke rnel.org/stabl e/c/3948abaa 4e2be938ccdf c289385a273 42fb13d43, https://git.ke rnel.org/stabl e/c/423b6bdf 19bbc5e1f7e7 46104509991 7378f7e71, https://git.ke rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228 a68d8a7c1	O-LIN-LINU- 030524/872

0-1

1-2

2-33-44-5Page 816 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_handle fs/fhandle.c:73 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517		
			do_kmalloc_node mm/slab_common.c:10 06 [inline]		
			_kmalloc+0x121/0x3c 0 mm/slab_common.c:10		
			20 kmalloc include/linux/slab.h:60 4 [inline]		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			do_sys_name_to_handle fs/fhandle.c:39 [inline]			
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]			
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94			
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94			
			Bytes 18-19 of 20 are uninitialized			
			Memory access of size 20 starts at ffff888128a46380			
			Data copied to user address 0000000020000240"			
			Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to			
			solve the problem.			
			CVE ID : CVE-2024- 26901			
Affected Ver	sion(s): From (i	ncluding)	3.10 Up to (excluding) 5.4	.273		
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/5c03387 021cfa3336b	O-LIN-LINU- 030524/873	
			net: ip_tunnel: make sure to pull inner	97e0dcba380 29917a8af2a,		
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 818 of 1051						

Page 818 of 1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header in ip_tunnel_rcv()	https://git.ke rnel.org/stabl e/c/60044ab	
			Apply the same fix than ones found in :	84836359534 bd7153b92e9 c1584140e4a,	
			8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in ip6_tnl_rcv()")	https://git.ke rnel.org/stabl e/c/77fd5294 ea09b21f677 2ac954a121b 87323cec80	
			1ca1ba465e55 ("geneve: make sure to pull inner header in geneve_rx()")		
			We have to save skb- >network_header in a temporary variable		
			in order to be able to recompute the network_header pointer		
			after a pskb_inet_may_pull() call.		
			pskb_inet_may_pull() makes sure the needed headers are in skb- >head.		
			syzbot reported:		
			BUG: KMSAN: uninit- value in INET_ECN_decapsulat		
			e include/net/inet_ecn.h: 253 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KMSAN: uninit- value in INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			BUG: KMSAN: uninit- value in IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			BUG: KMSAN: uninit- value in ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline] IP_ECN_decapsulate		
			include/net/inet_ecn.h: 302 [inline]		
			ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			ipgre_rcv+0x9bc/0xb c0 net/ipv4/ip_gre.c:389		
			ipgre_rcv net/ipv4/ip_gre.c:411 [inline]		
			gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447		

0-1

1-2

2-33-44-5Page 820 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c: 163		
			ip_protocol_deliver_rcu +0x264/0x1300 net/ipv4/ip_input.c:205		
			ip_local_deliver_finish+ 0x2b8/0x440 net/ipv4/ip_input.c:233 NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_local_deliver+0x21f/ 0x490 net/ipv4/ip_input.c:254		
			dst_input include/net/dst.h:461 [inline]		
			ip_rcv_finish net/ipv4/ip_input.c:449 [inline]		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569		
			netif_receive_skb_one _core net/core/dev.c:5534 [inline]		
			netif_receive_skb+0x1 a6/0x5a0 net/core/dev.c:5648		
			netif_receive_skb_intern		

0-1

1-2

2-33-44-5Page 821 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			al net/core/dev.c:5734 [inline]		
			netif_receive_skb+0x58 /0x660 net/core/dev.c:5793		
			tun_rx_batched+0x3ee/ 0x980 drivers/net/tun.c:1556		
			tun_get_user+0x53b9/0 x66e0 drivers/net/tun.c:2009		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		

0-1

1-2

2-33-44-5Page 822 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			Uninit was created at:		
			alloc_pages+0x9a6/0x e00 mm/page_alloc.c:4590		
			alloc_pages_mpol+0x62 b/0x9d0 mm/mempolicy.c:2133		
			alloc_pages+0x1be/0x1 e0 mm/mempolicy.c:2204		
			skb_page_frag_refill+0x 2bf/0x7c0 net/core/sock.c:2909		
			tun_build_skb drivers/net/tun.c:1686 [inline]		
			tun_get_user+0xe0a/0x 66e0 drivers/net/tun.c:1826		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		

0-1

1-2

2-33-44-5Page 823 of 1051

5-6

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
		call_write_iter include/linux/fs.h:2087 [inline]				
		new_sync_write fs/read_write.c:497 [inline]				
		vfs_write+0xb6b/0x15 20 fs/read_write.c:590				
		ksys_write+0x20f/0x4c 0 fs/read_write.c:643				
		do_sys_write fs/read_write.c:655 [inline]				
		se_sys_write fs/read_write.c:652 [inline]				
		x64_sys_write+0x93/ 0xd0 fs/read_write.c:652				
		do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]				
		do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm				
		on.c:83				
		entry_SYSCALL_64_afte r_hwframe+0x63/0x6b				
		CVE ID : CVE-2024- 26882				
Affected Version(s): From (including) 3.19 Up to (excluding) 4.19.311						
17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d	O-LIN-LINU- 030524/874		
	sion(s): From (i	sion(s): From (including)	includeincludeincludecall_write_iter include/linux/fs.h:2087 [inline]includenew_sync_write fs/read_write.c:497 [inline]vfs_write+0xb6b/0x15 20 fs/read_write.c:590ksys_write+0x20f/0x4c 0 fs/read_write.c:643 do_sys_write fs/read_write.c:655 [inline] se_sys_write fs/read_write.c:652 [inline] se_sys_write+0x93/ 0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83sion(s): From (including)3.19 Up to (excluding) 4.117-Apr-20247.8In the Linux kernel, the following vulnerability	call_write_iter include/linux/fs.h:2087 [inline]call_write.iter include/linux/fs.h:2087 [inline]new_sync_write fs/read_write.c:497 [inline]new_sync_write 		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			bpf: Fix hashtab overflow check on 32- bit arches	92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6 5f07b1132c1	
			The hashtab code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the	979d73f014a e6e04de55d, https://git.ke rnel.org/stabl e/c/64f00b4d f0597590b19 9b62a37a165 473bf658a6	
			resulting value is 0. However, on 32-bit arches, the roundup code itself		
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code. So apply the same		
			fix to hashtab, by moving the overflow check to before the roundup.		
			CVE ID : CVE-2024- 26884		
Affected Ver	sion(s): From (i	ncluding)	4.10 Up to (excluding) 4.1	4.295	

0-1

1-2

2-33-44-5Page 825 of 1051

5-6

6-7

7-8 8-9 9-10

N/A28-Apr-20245.5In the Linux kernel, the following vulnerability has been resolved:https://git.ke rel.org/stabl e/c/016b150 992eebc32c4 a187783c72bb 6c2543a30, https://git.ke rnel.org/stabl e/c/02bcd95 b241c20802e 9501940296, https://git.ke rnel.org/stabl e/c/02bcd95 b241c20802e 9501940296, https://git.ke rnel.org/stabl e/c/02bcd95 b241c20802e 9501940296, https://git.ke rnel.org/stabl e/c/02bcd95 b241c20802e 9501940296, https://git.ke rnel.org/stabl e/c/02bcd95 b241c20802e 9501940296, https://git.ke rnel.org/stabl e/c/2d6c55e 0c3804e1e2 27b80a5746e 086d6c6696c0-LIN-LINU- 030524/875N/A28-Apr-20245.5Internal error: Oops - BUC: 0 [#1] PREEMPT SMP0-LIN-LINU- 030524/875N/A28-Apr-20245.5Internal error: Oops - BUC: 0 [#1] PREEMPT SMP0-LIN-LINU- 030524/875Image: <b< th=""><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description &amp; CVE ID</th><th>Patch</th><th>NCIIPC ID</th></b<>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Call trace:https://git.ke rmel.org/stabl e/c/2d6e55e 0c03804e1e2 27b80a5746e 086d6c6696ckmem_cache_create+ 0x60/0x118 mm/slub.c:4899 create_cache mm/slab_common.c:22 9 [inline]https://git.ke rmel.org/stabl e/c/2d6e55e 0c03804e1e2 27b80a5746e 086d6c6696c				In the Linux kernel, the following vulnerability has been resolved: mm/slub: fix to return errno if kmalloc() fails In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to out-of-memory, if it fails, return errno correctly rather than triggering panic via BUG_ON(); kernel BUG at mm/slub.c:5893! Internal error: Oops - BUG: 0 [#1] PREEMPT	https://git.ke rnel.org/stabl e/c/016b150 992eebc32c4 a18f783cf2bb 6e2545a3d9, https://git.ke rnel.org/stabl e/c/02bcd95 1aa3c2cea95f b241c20802e	O-LIN-LINU-
rcopy+0x19c/0x31c mm/slab_common.c:33			sysfs_slab_add+0x258/ 0x260 mm/slub.c:5973 kmem_cache_create+ 0x60/0x118 mm/slub.c:4899 create_cache mm/slab_common.c:22 9 [inline] kmem_cache_create_use rcopy+0x19c/0x31c	rnel.org/stabl e/c/2d6e55e 0c03804e1e2 27b80a5746e		

0-1

1-2

2-33-44-5Page 826 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kmem_cache_create+0x 1c/0x28 mm/slab_common.c:39 0		
			f2fs_kmem_cache_creat e fs/f2fs/f2fs.h:2766 [inline]		
			f2fs_init_xattr_caches+0 x78/0xb4 fs/f2fs/xattr.c:808		
			f2fs_fill_super+0x1050/ 0x1e0c fs/f2fs/super.c:4149		
			mount_bdev+0x1b8/0x 210 fs/super.c:1400		
			f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512		
			legacy_get_tree+0x30/0 x74 fs/fs_context.c:610		
			vfs_get_tree+0x40/0x1 40 fs/super.c:1530		
			do_new_mount+0x1dc/ 0x4e4 fs/namespace.c:3040		
			path_mount+0x358/0x 914		
			fs/namespace.c:3370		
			do_mount fs/namespace.c:3383 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_mount fs/namespace.c:3591 [inline] se_sys_mount		
			fs/namespace.c:3568 [inline]		
			arm64_sys_mount+0x 2f8/0x408 fs/namespace.c:3568		
			CVE ID : CVE-2022- 48659		
Affected Ver	sion(s): From (i	ncluding)	4.15 Up to (excluding) 4.1	9.260	
			In the Linux kernel, the following vulnerability has been resolved:		
			mm/slub: fix to return errno if kmalloc() fails	https://git.ke rnel.org/stabl e/c/016b150 992eebc32c4	
			In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to	a18f783cf2bb 6e2545a3d9, https://git.ke	
N/A	28-Apr-2024 5.5	-Apr-2024 5.5	out-of-memory, if it fails, return errno correctly rather than	rnel.org/stabl e/c/02bcd95 1aa3c2cea95f b241c20802e 9501940296, https://git.ke rnel.org/stabl	0-LIN-LINU- 030524/876
			triggering panic via BUG_ON();		
			kernel BUG at mm/slub.c:5893!	e/c/2d6e55e 0c03804e1e2 27b80a5746e	
			Internal error: Oops - BUG: 0 [#1] PREEMPT SMP	086d6c6696c	
			Call trace:		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sysfs_slab_add+0x258/ 0x260 mm/slub.c:5973		
			kmem_cache_create+ 0x60/0x118 mm/slub.c:4899 create_cache mm/slab_common.c:22 9 [inline]		
			kmem_cache_create_use rcopy+0x19c/0x31c mm/slab_common.c:33 5		
			kmem_cache_create+0x 1c/0x28 mm/slab_common.c:39 0		
			f2fs_kmem_cache_creat e fs/f2fs/f2fs.h:2766 [inline]		
			f2fs_init_xattr_caches+0 x78/0xb4 fs/f2fs/xattr.c:808		
			f2fs_fill_super+0x1050/ 0x1e0c fs/f2fs/super.c:4149		
			mount_bdev+0x1b8/0x 210 fs/super.c:1400		
			f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512		
			legacy_get_tree+0x30/0 x74 fs/fs_context.c:610		

0-1

1-2

2-33-44-5Page 829 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_get_tree+0x40/0x1 40 fs/super.c:1530		
			do_new_mount+0x1dc/ 0x4e4		
			fs/namespace.c:3040		
			path_mount+0x358/0x 914 fs/namespace.c:3370		
			do_mount fs/namespace.c:3383 [inline]		
			do_sys_mount fs/namespace.c:3591 [inline]		
			se_sys_mount fs/namespace.c:3568 [inline]		
			arm64_sys_mount+0x 2f8/0x408 fs/namespace.c:3568		
			CVE ID : CVE-2022- 48659		
Affected Ver	sion(s): From (i	ncluding)	4.20 Up to (excluding) 5.4	.215	
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/016b150 992eebc32c4 a18f783cf2bb	
N/A	28-Apr-2024	5.5	mm/slub: fix to return errno if kmalloc() fails	6e2545a3d9, https://git.ke rnel.org/stabl e/c/02bcd95	O-LIN-LINU- 030524/877
			In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to	1aa3c2cea95f b241c20802e 9501940296, https://git.ke rnel.org/stabl	

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-memory, if it fails, return errno correctly rather than triggering panic via BUG_ON();	e/c/2d6e55e 0c03804e1e2 27b80a5746e 086d6c6696c	
			kernel BUG at mm/slub.c:5893! Internal error: Oops - BUG: 0 [#1] PREEMPT SMP		
			Call trace:		
			sysfs_slab_add+0x258/ 0x260 mm/slub.c:5973		
			kmem_cache_create+ 0x60/0x118 mm/slub.c:4899 create_cache mm/slab_common.c:22 9 [inline]		
			kmem_cache_create_use rcopy+0x19c/0x31c mm/slab_common.c:33 5		
			kmem_cache_create+0x 1c/0x28 mm/slab_common.c:39 0		
			f2fs_kmem_cache_creat e fs/f2fs/f2fs.h:2766 [inline]		
			f2fs_init_xattr_caches+0		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x78/0xb4 fs/f2fs/xattr.c:808		
			f2fs_fill_super+0x1050/ 0x1e0c fs/f2fs/super.c:4149		
			mount_bdev+0x1b8/0x 210 fs/super.c:1400 f2fs_mount+0x44/0x58		
			fs/f2fs/super.c:4512 legacy_get_tree+0x30/0 x74 fs/fs_context.c:610		
			vfs_get_tree+0x40/0x1 40 fs/super.c:1530		
			do_new_mount+0x1dc/ 0x4e4 fs/namespace.c:3040		
			path_mount+0x358/0x 914 fs/namespace.c:3370		
			do_mount fs/namespace.c:3383 [inline]		
			do_sys_mount fs/namespace.c:3591 [inline]		
			se_sys_mount fs/namespace.c:3568 [inline]		
			arm64_sys_mount+0x 2f8/0x408 fs/namespace.c:3568		
			CVE ID : CVE-2022- 48659		

0-1

1-2

2-33-44-5Page 832 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): From (i	ncluding)	4.20 Up to (excluding) 5.4	.273	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix stackmap overflow check on 32- bit arches The stackmap code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit arches, the roundup code itself can overflow by doing a 32-bit left-shift of an unsigned long value, which is undefined behaviour, so it is not guaranteed to truncate neatly. This was triggered by syzbot on the DEVMAP_HASH type, which contains the same check, copied from the hashtab code. The commit in the fixes tag actually attempted to fix this, but the fix did not account for the UB, so the fix only	https://git.ke rnel.org/stabl e/c/0971126 c8164abe200 4b8536b4969 0a0d6005b0a, https://git.ke rnel.org/stabl e/c/1564100 7df0f0d35fa2 8742b25c2a7 db9dcd6895, https://git.ke rnel.org/stabl e/c/21e5fa46 88e1a4d3db6 b72216231b2 4232f75c1d	0-LIN-LINU- 030524/878

0-1

1-2

2-33-44-5Page 833 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			works on CPUs where an		
			overflow does result in a neat truncation to zero, which is not		
			guaranteed. Checking the value before rounding does not have this		
			problem.		
			CVE ID : CVE-2024- 26883		
			In the Linux kernel, the following vulnerability has been resolved:		
		17-Apr-2024 7.8	bpf: Fix hashtab overflow check on 32- bit arches	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d 92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6 5f07b1132c1 979d73f014a e6e04de55d,	
Improper Restriction of Operations			The hashtab code relies on roundup_pow_of_two() to compute the number of		O-LIN-LINU-
within the Bounds of a Memory	17-Apr-2024		hash buckets, and contains an overflow check by checking if the		030524/879
Buffer		resulting value is 0. However, on 32-bit arches, the roundup code itself	https://git.ke rnel.org/stabl e/c/64f00b4d f0597590b19 9b62a37a165		
			can overflow by doing a 32-bit left-shift of an unsigned long value,	473bf658a6	
			which is undefined behaviour, so it is not guaranteed to truncate		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code. So apply the same		
			fix to hashtab, by moving the overflow check to before the roundup.		
			CVE ID : CVE-2024- 26884		
		17-Apr-2024 7.8	In the Linux kernel, the following vulnerability has been resolved:		
	17-Apr-2024 7.8		aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts	https://git.ke rnel.org/stabl e/c/079cba4f 4e307c69878 226fdf5228c2 0aa1c969c, https://git.ke rnel.org/stabl e/c/1a54aa50 6b3b2f31496 731039e4977 8f54eee881, https://git.ke rnel.org/stabl e/c/74ca3ef6 8d2f449bc84 8c0a814cefc4 87bf755fa	
Use After			This patch is against CVE-2023-6270. The description of cve is:		O-LIN-LINU-
Use After Free			A flaw was found in the ATA over Ethernet (AoE) driver in the Linux		030524/880
			kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on		
			`struct net_device`, and a use-after-free can be triggered by racing		
			between the free on the struct and the		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access through the `skbtxq`		
			global queue. This could lead to a denial of service condition or potential code		
			execution.		
			In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial		
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		
			This patch removed the dev_put(ifp) in the success path in		
			aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx().		
			CVE ID : CVE-2024- 26898		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialize d Resource	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak syzbot identified a kernel information leak vulnerability in do_sys_name_to_handle () and issued the following report [1]. [1] "BUG: KMSAN: kernel- infoleak in instrument_copy_to_use r include/linux/instrume nted.h:114 [inline] BUG: KMSAN: kernel- infoleak in _copy_to_user+0xbc/0x 100 lib/usercopy.c:40 instrument_copy_to_use r include/linux/instrume nted.h:114 [inline] _copy_to_user+0xbc/0x 100 lib/usercopy.c:40 copy_to_user include/linux/instrume nted.h:114 [inline] _copy_to_user include/linux/uaccess.h :191 [inline] do_sys_name_to_handle fs/fhandle.c:73 [inline]	https://git.ke rnel.org/stabl e/c/3948abaa 4e2be938ccdf c289385a273 42fb13d43, https://git.ke rnel.org/stabl e/c/423b6bdf 19bbc5e1f7e7 46104509991 7378f7e71, https://git.ke rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228 a68d8a7c1	O-LIN-LINU- 030524/881

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517		
			do_kmalloc_node mm/slab_common.c:10 06 [inline]		
			_kmalloc+0x121/0x3c 0 mm/slab_common.c:10 20		
			kmalloc include/linux/slab.h:60 4 [inline]		
			do_sys_name_to_handle fs/fhandle.c:39 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94 		
			Bytes 18-19 of 20 are uninitialized		
			Memory access of size 20 starts at ffff888128a46380		
			Data copied to user address 0000000020000240"		
			Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to		
			solve the problem.		
			CVE ID : CVE-2024- 26901		
NULL Pointer Dereferenc e	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/2535b84 8fa0f42ddff3e 5255cf5e742c	O-LIN-LINU-
	p. 2021		Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security	9b77bb26, https://git.ke rnel.org/stabl e/c/369f419c 097e82407dd	030524/882

0-1

1-2

**2-3** 3-4 4-5 Page **839** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			During our fuzz testing of the connection and disconnection process at the RFCOMM layer, we discovered this bug. By comparing the packets from a	429a202cde9 a73d3ae29b, https://git.ke rnel.org/stabl e/c/3ead59ba fad05f2967ae 2438c0528d5 3244cfde5	
			normal connection and disconnection process with the testcase that		
			triggered a KASAN report. We analyzed the cause of this bug as follows:		
			1. In the packets captured during a normal connection, the host sends a		
			`Read Encryption Key Size` type of `HCI_CMD` packet		
			(Command Opcode: 0x1408) to the controller to inquire the length of		
			encryption key.After receiving this packet, the controller immediately		
			replies with a Command Completepacket (Event Code: 0x0e) to return the		
			Encryption Key Size.		
			2. In our fuzz test case, the timing of the		

0-1

1-2

**2-3** 3-4 4-5 Page **840** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller's response to this		
			packet was delayed to an unexpected point: after the RFCOMM and L2CAP		
			layers had disconnected but before the HCI layer had disconnected.		
			3. After receiving the Encryption Key Size Response at the time described		
			in point 2, the host still called the rfcomm_check_security function.		
			However, by this time `struct l2cap_conn *conn = l2cap_pi(sk)- >chan->conn;`		
			had already been released, and when the function executed		
			`return hci_conn_security(conn ->hcon, d->sec_level, auth_type, d->out);`,		
			specifically when accessing `conn->hcon`, a null-ptr-deref error occurred.		
			To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling		
			rfcomm_recv_frame in rfcomm_process_rx.		

0-1

1-2

2-33-44-5Page 841 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 26903		
Affected Ver	sion(s): From (i	ncluding)	5.11 Up to (excluding) 5.1	5.149	
Affected Verse Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	sion(s): From (i 17-Apr-2024	ncluding) 4.7	26903	5.149 https://git.ke rnel.org/stabl e/c/653bc5e6 d9995d7d5f4 97c665b3218 75a626161c, https://git.ke rnel.org/stabl e/c/970709a 67696b100a5 7b33af1a3d7 5fc34b747eb, https://git.ke rnel.org/stabl e/c/97f7cf1cd 80eeed3b7c8 08b7c124632 95c751001	0-LIN-LINU- 030524/883
			rcu callback does not work: sets with timeout use garbage collectors		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions are split into two: cancelling garbage collectors safely at		
			executing the command received by netlink and moving the remaining		
			part only into the rcu callback.		
			CVE ID : CVE-2024- 26910		
Affected Ver	sion(s): From (i	ncluding)	5.11 Up to (excluding) 5.1	5.150	
			In the Linux kernel, the following vulnerability has been resolved:		
			pmdomain: mediatek: fix race conditions with genpd	https://git.ke rnel.org/stabl e/c/339ddc9	
Concurrent Execution using			If the power domains are registered first with genpd and *after that*	83bc1622341 d95f244c361c da3da3a4ff, https://git.ke rnel.org/stabl e/c/3cd1d92e e1dbf3e8f988 767eb75f262 07397792b, https://git.ke rnel.org/stabl e/c/475426a	
Shared Resource with Improper	17-Apr-2024	17-Apr-2024 4.7	the driver attempts to power them on in the probe sequence, then it is		0-LIN-LINU- 030524/884
Synchroniz ation ('Race Condition')			possible that a race condition occurs if genpd tries to power them on		
			in the same time.	d1ae0bfdfd8f 160ed975090	
		The same is valid for powering them off before unregistering them	3799392438		
			from genpd.		
			Attempt to fix race conditions by first		

0-1

1-2

2-33-44-5Page 843 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the domains from genpd		
			and *after that* powering down domains.		
			Also first power up the domains and *after that* register them		
			to genpd.		
			CVE ID : CVE-2023- 52645		
Affected Ver	sion(s): From (i	ncluding)	5.11 Up to (excluding) 5.1	5.153	
			In the Linux kernel, the following vulnerability has been resolved:		
			net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv()	https://git.ke rnel.org/stabl e/c/5c03387 021cfa3336b	
			Apply the same fix than ones found in :	97e0dcba380 29917a8af2a, https://git.ke rnel.org/stabl	
N/A	17-Apr-2024 7.8	17-Apr-2024 7.8	8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in ip6_tnl_rcv()")	e/c/60044ab 84836359534 bd7153b92e9 c1584140e4a, https://git.ke	O-LIN-LINU- 030524/885
			1ca1ba465e55 ("geneve: make sure to pull inner header in geneve_rx()")	rnel.org/stabl e/c/77fd5294 ea09b21f677 2ac954a121b 87323cec80	
			We have to save skb- >network_header in a temporary variable		
			in order to be able to recompute the		

0-1

1-2

**2-3** 3-4 4-5 Page **844** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network_header pointer		
			after a pskb_inet_may_pull() call.		
			pskb_inet_may_pull() makes sure the needed headers are in skb- >head.		
			syzbot reported:		
			BUG: KMSAN: uninit- value in INET_ECN_decapsulat e include/net/inet_ecn.h: 252 [inline]		
			253 [inline] BUG: KMSAN: uninit-		
			value in INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			BUG: KMSAN: uninit- value in IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			BUG: KMSAN: uninit- value in ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		

0-1

1-2

2-33-44-5Page 845 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			ipgre_rcv+0x9bc/0xb c0 net/ipv4/ip_gre.c:389		
			ipgre_rcv net/ipv4/ip_gre.c:411 [inline]		
			gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447		
			gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c: 163		
			ip_protocol_deliver_rcu +0x264/0x1300 net/ipv4/ip_input.c:205		
			ip_local_deliver_finish+ 0x2b8/0x440 net/ipv4/ip_input.c:233		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_local_deliver+0x21f/ 0x490 net/ipv4/ip_input.c:254		

0-1

1-2

**2-3** 3-4 4-5 Page **846** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dst_input include/net/dst.h:461 [inline]		
			ip_rcv_finish net/ipv4/ip_input.c:449 [inline]		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569		
			netif_receive_skb_one _core net/core/dev.c:5534 [inline]		
			netif_receive_skb+0x1 a6/0x5a0 net/core/dev.c:5648		
			netif_receive_skb_intern al net/core/dev.c:5734 [inline]		
			netif_receive_skb+0x58 /0x660 net/core/dev.c:5793		
			tun_rx_batched+0x3ee/ 0x980 drivers/net/tun.c:1556		
			tun_get_user+0x53b9/0 x66e0 drivers/net/tun.c:2009		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			Uninit was created at:		
			alloc_pages+0x9a6/0x e00 mm/page_alloc.c:4590		
			mm/ page_anoc.c.4370		

0-1

1-2

5-6

6-7

7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alloc_pages_mpol+0x62 b/0x9d0 mm/mempolicy.c:2133		
			alloc_pages+0x1be/0x1 e0 mm/mempolicy.c:2204		
			skb_page_frag_refill+0x 2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline]		
			tun_get_user+0xe0a/0x 66e0 drivers/net/tun.c:1826		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643 do_sys_write		
			fs/read_write.c:655 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			CVE ID : CVE-2024- 26882		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/0971126	
Improper Restriction of			bpf: Fix stackmap overflow check on 32- bit arches	c8164abe200 4b8536b4969 0a0d6005b0a, https://git.ke rnel.org/stabl	
Operations within the Bounds of a Memory	17-Apr-2024	7.8	The stackmap code relies on roundup_pow_of_two() to compute the number	e/c/1564100 7df0f0d35fa2 8742b25c2a7 db9dcd6895,	0-LIN-LINU- 030524/886
Buffer			of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit	https://git.ke rnel.org/stabl e/c/21e5fa46 88e1a4d3db6 b72216231b2	
			arches, the roundup code itself	4232f75c1d	

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code.		
			The commit in the fixes tag actually attempted to fix this, but the fix		
			did not account for the UB, so the fix only works on CPUs where an		
			overflow does result in a neat truncation to zero, which is not		
			guaranteed. Checking the value before rounding does not have this		
			problem.		
			CVE ID : CVE-2024- 26883		
Improper Restriction of			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d	O-LIN-LINU-
Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	bpf: Fix hashtab overflow check on 32- bit arches	92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6	030524/887

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The hashtab code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit arches, the roundup code itself	5f07b1132c1 979d73f014a e6e04de55d, https://git.ke rnel.org/stabl e/c/64f00b4d f0597590b19 9b62a37a165 473bf658a6	
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code. So apply the same		
			fix to hashtab, by moving the overflow check to before the roundup.		
			CVE ID : CVE-2024- 26884		
Improper Restriction of Operations	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/22079b3 a423382335f 47d9ed32114	O-LIN-LINU-
within the Bounds of a Memory Buffer	27 Hpt 2021		bpf: Fix DEVMAP_HASH overflow check on 32- bit arches	e6c9fe88d7c, https://git.ke rnel.org/stabl e/c/225da02	030524/888

0-1

1-2

2-33-44-5Page 852 of 1051

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The devmap code allocates a number hash buckets equal to the next power	acdc97af01b6 bc6ce1a3e53 62bf01d3fb, https://git.ke	
			of two of the max_entries value provided when creating the map. When	rnel.org/stabl e/c/250051ac c21f9d4c5c59 5e4fcb55986e	
			rounding up to the next power of two, the 32-bit variable storing the	a08c4691	
			number of buckets can overflow, and the code checks for overflow by		
			checking if the truncated 32-bit value is equal to 0. However, on 32-bit		
			arches the rounding up itself can overflow mid- way through, because it		
			ends up doing a left- shift of 32 bits on an unsigned long value. If the		
			size of an unsigned long is four bytes, this is undefined behaviour, so		
			there is no guarantee that we'll end up with a nice and tidy 0-value at		
			the end.		
			Syzbot managed to turn this into a crash on arm32 by creating a		
			DEVMAP_HASH with max_entries > 0x80000000 and then trying to update it.		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix this by moving the overflow check to before the rounding up		
			operation.		
			CVE ID : CVE-2024- 26885		
			In the Linux kernel, the following vulnerability has been resolved:		
			aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts		
Use After Free 17-Apr-2024		r-2024 <b>7.8</b>	<ul> <li>.7-Apr-2024</li> <li>7.8</li> <li>description of cve is:</li> <li>e/c/079cba4f 4e307c69878 226fdf5228c2 0aa1c969c, https://git.ke rnel.org/stabl e/c/1a54aa50 6b3b2f31496</li> </ul>	rnel.org/stabl e/c/079cba4f	
	17-Apr-2024			7.8	7.8
			function improperly 8f.	8f54eee881, https://git.ke	
			`struct net_device`, and a use-after-free can be triggered by racing	rnel.org/stabl e/c/74ca3ef6 8d2f449bc84 8c0a814cefc4 87bf755fa	
			between the free on the struct and the access through the `skbtxq`		
		global queue. This could lead to a denial of service condition or			
		potential code execution.			

0-1

1-2

2-33-44-5Page 854 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial		
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		
			This patch removed the dev_put(ifp) in the success path in		
			aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx().		
			CVE ID : CVE-2024- 26898		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/185fa070 00e0a81d54cf	
N/A	17-Apr-2024	7.8	RDMA/mlx5: Fix fortify source warning while accessing Eth segment	8c05414cebff 14469a5c, https://git.ke rnel.org/stabl e/c/4d5e86a	O-LIN-LINU- 030524/890
			[ cut here ]	56615cc387d 21c629f9af8f b0e958d350,	

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131 (size 2)	https://git.ke rnel.org/stabl e/c/60ba938 a8bc8c90e72 4c75f98e932f 9fb7ae1b9d	
			WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131 mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			Modules linked in: 8021q garp mrp stp llc rdma_ucm(OE) rdma_cm(OE) ib_ipoib(OE) ib_cm(OE) ib_umad(OE) mlx5_ib(OE) ib_uverbs(OE) ib_core(OE) mlx5_core(OE) pci_hyperv_intf mlxdevm(OE)		
			mlx_compat(OE) tls mlxfw(OE) psample nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip_set nf_tables libcrc32c		

0-1

1-2

**2-3** 3-4 4-5 Page **856** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	nfnetlink mst_pciconf(OE) knem(OE) vfio_pci vfio_pci_core vfio_iommu_type1 vfio iommufd irqbypass cuse nfsv3 nfs fscache netfs xfrm_user xfrm_algo ipmi_devintf ipmi_msghandler binfmt_misc crct10dif_pclmul crc32_pclmul polyval_clmulni polyval_generic ghash_clmulni_intel sha512_ssse3 snd_pcsp aesni_intel crypto_simd cryptd snd_pcm snd_timer joydev snd soundcore input_leds serio_raw evbug nfsd auth_rpcgss nfs_acl lockd grace	Patch	NCIIPC ID
			sch_fq_codel sunrpc drm efi_pstore ip_tables x_tables autofs4 psmouse virtio_net net_failover failover floppy		
			[last unloaded: mlx_compat(OE)] CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2.0-32-generic #32~22.04.1-Ubuntu		
			Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 RIP: 0010:mlx5_ib_post_sen		

0-1

1-2

2-33-44-5Page 857 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d+0x191b/0x1a60 [mlx5_ib]		
			Code: 0c 01 00 a8 01 75 25 48 8b 75 a0 b9 02		
			00 00 00 48 c7 c2 10 5b		
			fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01		
			e8 95 4d 93 da <0f> 0b		
			44 8b 4d b0 4c 8b 45 c8 48 8b 4d c0 e9 49 fb ff ff 41 0f b7		
			RSP:		
			0018:ffffb5b48478b570 EFLAGS: 00010046		
			RAX: 00000000000000000 RBX:		
			000000000000000000000000000000000000000		
			RCX: 00000000000000000		
			RDX: 00000000000000000 RSI:		
			00000000000000000 RDI: 0000000000000000000000		
			RBP: ffffb5b48478b628 R08: 00000000000000000 R09: 000000000000000		
			R10: 00000000000000000000000		
			R11: 00000000000000000000 R12: ffffb5b48478b5e8		
			R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80		
			FS: 00007fc03b444c80(00		

0-1

1-2

**2-3** 3-4 4-5 Page **858** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00) GS:ffff963a3dc00000(0 000) knlGS:0000000000000 000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			CR2: 0000556f46bdf000 CR3: 000000006ac6003 CR4: 0000000003706f0		
			DR0: 000000000000000000 DR1: 00000000000000000 DR2: 000000000000000000000000000000000000		
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		
			<task> 2</task>		
			? show_regs+0x72/0x90		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?_warn+0x8d/0x160		
			? mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?		
			report_bug+0x1bb/0x1 d0		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? handle_bug+0x46/0x90 ?		
			exc_invalid_op+0x19/0 x80		
			? asm_exc_invalid_op+0x 1b/0x20		
			? mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			mlx5_ib_post_send_nod rain+0xb/0x20 [mlx5_ib]		
			ipoib_send+0x2ec/0x77 0 [ib_ipoib]		
			ipoib_start_xmit+0x5a0 /0x770 [ib_ipoib]		
			dev_hard_start_xmit+0x 8e/0x1e0		
			? validate_xmit_skb_list+ 0x4d/0x80		
			sch_direct_xmit+0x116 /0x3a0		
			dev_xmit_skb+0x1fd/ 0x580		
			dev_queue_xmit+0x28 4/0x6b0 ?		
			; _raw_spin_unlock_irq+0 xe/0x50		

0-1

1-2

3-4 4-5 2-3

6-7 8-9 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? flush_work.isra.0+0x2 0d/0x370 ?		
			ہ push_pseudo_header+0 x17/0x40 [ib_ipoib]		
			neigh_connected_outpu t+0xcd/0x110		
			ip_finish_output2+0x17 9/0x480		
			? smp_call_single_queue +0x61/0xa0		
			ip_finish_output+0xc3 /0x190		
			ip_finish_output+0x2e/ 0xf0		
			ip_output+0x78/0x110 ?		
			pfx_ip_finish_output+ 0x10/0x10		
			ip_local_out+0x64/0x7 0		
			ip_queue_xmit+0x18a /0x460		
			ip_queue_xmit+0x15/0 x30		
			tcp_transmit_skb+0x9 14/0x9c0		

0-1

1-2

3-4 4-5 2-3 Page 861 of 1051

7-8 8-9 9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_write_xmit+0x334/ 0x8d0		
			tcp_push_one+0x3c/0x 60		
			tcp_sendmsg_locked+0x 2e1/0xac0		
			tcp_sendmsg+0x2d/0x5 0		
			inet_sendmsg+0x43/0x 90		
			sock_sendmsg+0x68/0x 80		
			sock_write_iter+0x93/0 x100		
			vfs_write+0x326/0x3c0		
			ksys_write+0xbd/0xf0		
			? do_syscall_64+0x69/0x 90		
			x64_sys_write+0x19/ 0x30		
			do_syscall_		
			truncated <b>CVE ID : CVE-2024-</b>		
			26907		
Use of Uninitialize d Resource	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/3948abaa 4e2be938ccdf c289385a273	O-LIN-LINU- 030524/891

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak	42fb13d43, https://git.ke rnel.org/stabl e/c/423b6bdf	
			syzbot identified a kernel information leak vulnerability in	19bbc5e1f7e7 46104509991 7378f7e71, https://git.ke	
			do_sys_name_to_handle () and issued the following report [1].	rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228	
			[1]	a68d8a7c1	
			"BUG: KMSAN: kernel- infoleak in		
			instrument_copy_to_use r		
			include/linux/instrume nted.h:114 [inline]		
			BUG: KMSAN: kernel- infoleak in		
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40		
			instrument_copy_to_use r		
			include/linux/instrume nted.h:114 [inline]		
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40		
			copy_to_user include/linux/uaccess.h :191 [inline]		
			do_sys_name_to_handle fs/fhandle.c:73 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			 Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517		
			do_kmalloc_node mm/slab_common.c:10 06 [inline]		
			kmalloc+0x121/0x3c 0 mm/slab_common.c:10 20		
			kmalloc include/linux/slab.h:60 4 [inline]		
			do_sys_name_to_handle fs/fhandle.c:39 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Bytes 18-19 of 20 are uninitialized		
			Memory access of size 20 starts at ffff888128a46380		
			Data copied to user address 0000000020000240"		
			Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to		
			solve the problem.		
			CVE ID : CVE-2024- 26901		
	17-Apr-2024 5.5		In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/2535b84 8fa0f42ddff3e	
NULL Pointer Dereferenc e		5.5	Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security	5255cf5e742c 9b77bb26, https://git.ke rnel.org/stabl e/c/369f419c	O-LIN-LINU- 030524/892
			During our fuzz testing of the connection and disconnection process at the	097e82407dd 429a202cde9 a73d3ae29b, https://git.ke rnel.org/stabl	

0-1

1-2

2-33-44-5Page 865 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RFCOMM layer, we discovered this bug. By comparing the packets from a	e/c/3ead59ba fad05f2967ae 2438c0528d5 3244cfde5	
			normal connection and disconnection process with the testcase that		
			triggered a KASAN report. We analyzed the cause of this bug as follows:		
			1. In the packets captured during a normal connection, the host sends a		
			`Read Encryption Key Size` type of `HCI_CMD` packet		
			(Command Opcode: 0x1408) to the controller to inquire the length of		
			encryption key.After receiving this packet, the controller immediately		
			replies with a Command Completepacket (Event Code: 0x0e) to return the		
			Encryption Key Size.		
			2. In our fuzz test case, the timing of the controller's response to this		
			packet was delayed to an unexpected point:		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			after the RFCOMM and L2CAP					
			layers had disconnected but before the HCI layer had disconnected.					
			3. After receiving the Encryption Key Size Response at the time described					
			in point 2, the host still called the rfcomm_check_security function.					
			However, by this time `struct l2cap_conn *conn = l2cap_pi(sk)- >chan->conn;`					
			had already been released, and when the function executed					
			`return hci_conn_security(conn ->hcon, d->sec_level, auth_type, d->out);`,					
			specifically when accessing `conn->hcon`, a null-ptr-deref error occurred.					
			To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling					
			rfcomm_recv_frame in rfcomm_process_rx.					
			CVE ID : CVE-2024- 26903					
Affected Ver	Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.71							

0-1

1-2

 2-3
 3-4
 4-5

 Page 867 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness N/A	Publish Date	<b>CVSSv3</b>	Description & CVE ID In the Linux kernel, the following vulnerability has been resolved: mm/slub: fix to return errno if kmalloc() fails In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to out-of-memory, if it fails, return errno correctly rather than triggering panic via BUG_ON(); kernel BUG at mm/slub.c:5893! Internal error: Oops - BUG: 0 [#1] PREEMPT SMP	Patch https://git.ke rnel.org/stabl e/c/016b150 992eebc32c4 a18f783cf2bb 6e2545a3d9, https://git.ke rnel.org/stabl e/c/02bcd95 1aa3c2cea95f b241c20802e 9501940296, https://git.ke	NCIIPC ID
			Call trace: sysfs_slab_add+0x258/ 0x260 mm/slub.c:5973 kmem_cache_create+	rnel.org/stabl e/c/2d6e55e 0c03804e1e2 27b80a5746e 086d6c6696c	
			0x60/0x118 mm/slub.c:4899		
			create_cache mm/slab_common.c:22 9 [inline]		
			kmem_cache_create_use rcopy+0x19c/0x31c mm/slab_common.c:33 5		

0-1

1-2

**2-3** 3-4 4-5 Page **868** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kmem_cache_create+0x 1c/0x28 mm/slab_common.c:39 0		
			f2fs_kmem_cache_creat e fs/f2fs/f2fs.h:2766 [inline]		
			f2fs_init_xattr_caches+0 x78/0xb4 fs/f2fs/xattr.c:808		
			f2fs_fill_super+0x1050/ 0x1e0c fs/f2fs/super.c:4149		
			mount_bdev+0x1b8/0x 210 fs/super.c:1400		
			f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512		
			legacy_get_tree+0x30/0 x74 fs/fs_context.c:610		
			vfs_get_tree+0x40/0x1 40 fs/super.c:1530		
			do_new_mount+0x1dc/ 0x4e4 fs/namespace.c:3040		
			path_mount+0x358/0x 914		
			fs/namespace.c:3370		
			do_mount fs/namespace.c:3383 [inline]		

0-1

1-2

**2-3** 3-4 4-5 Page **869** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_mount fs/namespace.c:3591 [inline] se_sys_mount		
			fs/namespace.c:3568 [inline] arm64_sys_mount+0x		
			2f8/0x408 fs/namespace.c:3568		
			CVE ID : CVE-2022- 48659		
			In the Linux kernel, the following vulnerability has been resolved:		
			gpiolib: cdev: Set lineevent_state::irq after IRQ register successfully	https://git.ke rnel.org/stabl e/c/657803b 918e097e47d 99d1489da83	
			When running gpio test on nxp-ls1028 platform with below command	a603c36bcdd, https://git.ke rnel.org/stabl	O-LIN-LINU- 030524/894
N/A	28-Apr-2024	4 5.5	gpiomonnum- events=3rising-edge gpiochip1 25	e/c/69bef19d 6b9700e9628 5f4b4e28691 cda3dcd0d1, https://git.ke rnel.org/stabl	
			There will be a warning trace as below:		
			Call trace: free_irq+0x204/0x360	e/c/97da736c d11ae73bdf2f	
			lineevent_free+0x64/0x 70	5e21e24446b 8349e0168	
			gpio_ioctl+0x598/0x6a 0		
			_arm64_sys_ioctl+0xb4 /0x100		

0-1

1-2

2-33-44-5Page 870 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoke_syscall+0x5c/0x 130		
			el0t_64_sync+0x1a0/0x 1a4		
			The reason of this issue is that calling request_threaded_irq()		
			function failed, and then lineevent_free() is invoked to release		
			the resource. Since the lineevent_state::irq was already set, so		
			the subsequent invocation of free_irq() would trigger the above		
			warning call trace. To fix this issue, set the lineevent_state::irq		
			after the IRQ register successfully.		
			CVE ID : CVE-2022- 48660		
Affected Ver	sion(s): From (i	ncluding)	5.14 Up to (excluding) 5.1	5.153	
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/0fbcf236 6ba9888cf02e da23e35fde7f	
NULL Pointer Dereferenc e	17-Apr-2024	5.5	net: hns3: fix kernel crash when 1588 is received on HIP08 devices	7fcc07c3, https://git.ke rnel.org/stabl e/c/11b9983 60d96f6c76f0	O-LIN-LINU- 030524/895
			The HIP08 devices does not register the ptp devices, so the	4a95f54b49f2 4d3c858e4, https://git.ke rnel.org/stabl e/c/23ec1cec	

0-1

1-2

2-33-44-5Page 871 of 1051

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hdev->ptp is NULL, but the hardware can receive 1588 messages,	24293f9799c 725941677d4 e167997265	
			and set the HNS3_RXD_TS_VLD_B bit, so, if match this case, the		
			access of hdev->ptp- >flags will cause a kernel crash:		
			[ 5888.946472] Unable to handle kernel NULL pointer dereference at virtual address 000000000000018		
			[ 5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 00000000000018		
			 [ 5889.266118] pc : hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.272612] lr : hclge_ptp_get_rx_hwts+ 0x34/0x170 [hclge]		
			[ 5889.279101] sp : ffff800012c3bc50		
			[ 5889.283516] x29: ffff800012c3bc50 x28: ffff2040002be040		
			[ 5889.289927] x27: ffff800009116484 x26: 0000000080007500		
			[ 5889.296333] x25: 00000000000000000 x24: ffff204001c6f000		

0-1

1-2

2-33-44-5Page 872 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.302738] x23: ffff204144f53c00 x22: 00000000000000000		
			[ 5889.309134] x21: 0000000000000000 x20: ffff204004220080		
			[ 5889.315520] x19: ffff204144f53c00 x18: 00000000000000000		
			[ 5889.321897] x17: 00000000000000000 x16:		
			0000000000000000 [ 5889.328263] x15: 0000004000140ec8 x14: 00000000000000000000000		
			[ 5889.334617] x13: 00000000000000000 x12: 00000000010011df		
			[ 5889.340965] x11: bbfeff4d22000000 x10: 000000000000000000		
			[ 5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d		
			[ 5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480		
			[ 5889.359959] x5 : 0000000000000000 x4 : 000000000000000000		
			[ 5889.366271] x3 : 000000000000000 x2 : 00000000000000000		
			[ 5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		

0-1

1-2

2-33-44-5Page 873 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.378857] Call trace:		
			[ 5889.382285] hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.388304] hns3_handle_bdinfo+0x 324/0x410 [hns3]		
			[ 5889.394055] hns3_handle_rx_bd+0x6 0/0x150 [hns3]		
			[ 5889.399624] hns3_clean_rx_ring+0x8 4/0x170 [hns3]		
			[ 5889.405270] hns3_nic_common_poll +0xa8/0x220 [hns3]		
			[ 5889.411084] napi_poll+0xcc/0x264		
			[ 5889.415329] net_rx_action+0xd4/0x 21c		
			[ 5889.419911] do_softirq+0x130/0x 358		
			[ 5889.424484] irq_exit+0x134/0x154		
			[ 5889.428700] handle_domain_irq+0 x88/0xf0		
			[ 5889.433684] gic_handle_irq+0x78/0 x2c0		
			[ 5889.438319] el1_irq+0xb8/0x140		
			[ 5889.442354] arch_cpu_idle+0x18/0x 40		

0-1

1-2

2-33-44-5Page 874 of 1051

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.446816] default_idle_call+0x5c/ 0x1c0		
			[ 5889.451714] cpuidle_idle_call+0x174 /0x1b0		
			[ 5889.456692] do_idle+0xc8/0x160		
			[ 5889.460717] cpu_startup_entry+0x3 0/0xfc		
			[ 5889.465523] secondary_start_kernel +0x158/0x1ec		
			[ 5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80)		
			[ 5889.477950] SMP: stopping secondary CPUs		
			[ 5890.514626] SMP: failed to stop secondary CPUs 0-69,71-95		
			[ 5890.522951] Starting crashdump kernel		
			CVE ID : CVE-2024- 26881		
Affected Ver	sion(s): From (i	ncluding)	5.15 Up to (excluding) 5.1	5.71	
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/713fa3e4 591f65f804bd c88e8648e21	0.1.11.1.11.11
N/A	28-Apr-2024	7.8	drm/i915/gem: Really move i915_gem_context.link under ref protection	9fabc9ee1, https://git.ke rnel.org/stabl e/c/d119888 b09bd567e07 c6b93a07f17	0-LIN-LINU- 030524/896

0-1

1-2

2-33-44-5Page 875 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			i915_perf assumes that it can use the i915_gem_context reference to	5df88857e02, https://git.ke rnel.org/stabl e/c/f799e056	
			protect its i915- >gem.contexts.list iteration. However, this requires	8d6c153368b 177e0bbbde7 dcc4ce7f1d	
			that we do not remove the context from the list until after we drop the		
			final reference and release the struct. If, as currently, we remove the		
			context from the list during context_close(), the link.next pointer may		
			be poisoned while we are holding the context reference and cause a GPF:		
			[ 4070.573157] i915 0000:00:02.0: [drm:i915_perf_open_io ctl [i915]] filtering on ctx_id=0x1fffff ctx_id_mask=0x1fffff		
			[ 4070.574881] general protection fault, probably for non- canonical address 0xdead000000000100: 0000 [#1] PREEMPT SMP		
			[ 4070.574897] CPU: 1 PID: 284392 Comm: amd_performance		

0-1

1-2

2-33-44-5Page 876 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tainted: G E 5.17.9 #180		
			[ 4070.574903] Hardware name: Intel Corporation		
			NUC7i5BNK/NUC7i5BN B, BIOS BNKBL357.86A.0052.2 017.0918.1346 09/18/2017		
			[ 4070.574907] RIP: 0010:oa_configure_all_c ontexts.isra.0+0x222/0 x350 [i915]		
			[ 4070.574982] Code: 08 e8 32 6e 10 e1 4d 8b 6d 50 b8 ff ff ff ff 49 83 ed 50 f0 41 0f c1 04 24 83 f8 01 0f 84 e3 00 00 00 85 c0 0f 8e fa 00 00 00 <49> 8b 45 50 48 8d 70 b0 49 8d 45 50 48 39 44 24 10 0f 85 34 fe		
			ff [ 4070.574990] RSP: 0018:ffffc90002077b78 EFLAGS: 00010202		
			[ 4070.574995] RAX: 0000000000000002 RBX: 00000000000000002 RCX: 0000000000000000000		
			[ 4070.575000] RDX: 000000000000000001 RSI: ffffc90002077b20 RDI: ffff88810ddc7c68		
			[ 4070.575004] RBP: 00000000000000001 R08: ffff888103242648 R09: fffffffffffffff		

0-1

1-2

2-33-44-5Page 877 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 4070.575008] R10: ffffffff82c50bc0 R11: 0000000000025c80 R12: ffff888101bf1860		
			[ 4070.575012] R13: dead000000000000000 R14: ffffc90002077c04 R15: ffff88810be5cabc		
			[ 4070.575016] FS: 00007f1ed50c0780(00 00) GS:ffff888885ec80000(0 000) knlGS:0000000000000 000		
			[ 4070.575021] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			[ 4070.575025] CR2: 00007f1ed5590280 CR3: 000000010ef6f005 CR4: 0000000003706e0		
			[ 4070.575029] Call Trace:		
			[ 4070.575033] <task></task>		
			[ 4070.575037] lrc_configure_all_contex ts+0x13e/0x150 [i915]		
			[ 4070.575103] gen8_enable_metric_set +0x4d/0x90 [i915]		
			[ 4070.575164] i915_perf_open_ioctl+0 xbc0/0x1500 [i915]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4070.575224] ? asm_common_interrupt +0x1e/0x40		
			[ 4070.575232] ? i915_oa_init_reg_state+ 0x110/0x110 [i915]		
			[ 4070.575290] drm_ioctl_kernel+0x85 /0x110		
			[ 4070.575296] ? update_load_avg+0x5f/ 0x5e0		
			[ 4070.575302] drm_ioctl+0x1d3/0x37 0		
			[ 4070.575307] ? i915_oa_init_reg_state+ 0x110/0x110 [i915]		
			[ 4070.575382] ? gen8_gt_irq_handler+0x 46/0x130 [i915]		
			[ 4070.575445] x64_sys_ioctl+0x3c4/ 0x8d0		
			[ 4070.575451] ? do_softirq+0xaa/0x1d 2		
			[ 4070.575456] do_syscall_64+0x35/0x 80		
			[ 4070.575461] entry_SYSCALL_64_afte r_hwframe+0x44/0xae		
			[ 4070.575467] RIP: 0033:0x7f1ed5c10397		
			[ 4070.575471] Code: 3c 1c e8 1c ff ff ff 85 c0 79 87 49 c7 c4 ff ff ff ff		
			5b 5d 4c 89 e0 41 5c c3 66 0f 1f 84 00 00 00 00		

0-1

1-2

2-33-44-5Page 879 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00 b8 10 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d a9 da 0d 00 f7 d8 64 89 01 48		
			[ 4070.575478] RSP: 002b:00007ffd65c8d7a 8 EFLAGS: 00000246 ORIG_RAX: 000000000000010		
			[ 4070.575484] RAX: fffffffffffffffda RBX: 00000000000000000 RCX: 00007f1ed5c10397		
			[ 4070.575488] RDX: 00007ffd65c8d7c0 RSI: 0000000040106476 RDI: 0000000000000000006		
			[ 4070.575492] RBP: 00005620972f9c60 R08: 0000000000000000a R09:		
			00000000000000005 [ 4070.575496] R10: 0000000000000000 R11:		
			R11: 0000000000000246 R12: 000000000000000000000000000000000000		
			[ 4070.575500] R13: 00000000000000000 R14: 00000000000000000000000		
			R15: 00007ffd65c8d7c0		
			[ 4070.575505] 		
			[ 4070.575507] Modules linked in:		

0-1

1-2

**2-3** 3-4 4-5 Page **880** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nls_ascii(E) nls_cp437(E) vfat(E) fat(E) i915(E) x86_pkg_temp_thermal( E) intel_powerclamp(E) crct10dif_pclmul(E) crc32_pclmul(E) crc32c_intel(E) aesni_intel(E) crypto_simd(E) intel_gtt(E) cryptd(E) ttm(E) rapl(E) intel_cstate(E) drm_kms_helper(E) cfbfillrect(E) syscopyarea(E) cfbimgblt(E) intel_uncore(E) sysfillrect(E) mei_me(E) sysimgblt(E) i2c_i801(E) fb_sys_fops(E) mei(E) intel_pch_thermal(E) i2c_smbus		
			truncated CVE ID : CVE-2022- 48662		
Improper Resource Shutdown or Release	28-Apr-2024	5.5	48662In the Linux kernel, the following vulnerability has been resolved:gpio: mockup: Fix potential resource leakage when register a chipIf creation of software node fails, the locally allocated string array is left unfreed. Free it on error path.	https://git.ke rnel.org/stabl e/c/02743c4 091ccfb246f5 cdbbe3f44b1 52d5d12933, https://git.ke rnel.org/stabl e/c/41f85703 3c44442a27f 591fda8d986 e7c9e42872, https://git.ke rnel.org/stabl e/c/9b26723 e058faaf11b5	O-LIN-LINU- 030524/897

0-1

1-2

2-33-44-5Page 881 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022- 48661	32fb4aa16d6 849d581790	
Affected Ver	sion(s): From (i	ncluding)	5.16 Up to (excluding) 5.1	9.12	
Affected Ver	sion(s): From (i 28-Apr-2024	ncluding) 7.8	<ul> <li>5.16 Up to (excluding) 5.1</li> <li>In the Linux kernel, the following vulnerability has been resolved:</li> <li>drm/i915/gem: Really move i915_gem_context.link under ref protection</li> <li>i915_perf assumes that it can use the i915_gem_context reference to protect its i915-&gt;gem.contexts.list iteration. However, this requires</li> <li>that we do not remove the context from the list until after we drop the final reference and release the struct. If, as currently, we remove the context from the list during context_close(), the link.next pointer may</li> <li>be poisoned while we are holding the context reference and cause a GPF:</li> </ul>	9.12 https://git.ke rnel.org/stabl e/c/713fa3e4 591f65f804bd c88e8648e21 9fabc9ee1, https://git.ke rnel.org/stabl e/c/d119888 b09bd567e07 c6b93a07f17 5df88857e02, https://git.ke rnel.org/stabl e/c/f799e056 8d6c153368b 177e0bbbde7 dcc4ce7f1d	O-LIN-LINU- 030524/898

0-1

1-2

2-33-44-5Page 882 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ctx_id=0x1fffff ctx_id_mask=0x1fffff [ 4070.574881] general protection fault, probably for non- canonical address 0xdead000000000100: 0000 [#1] PREEMPT SMP		
			[ 4070.574897] CPU: 1 PID: 284392 Comm: amd_performance Tainted: G E 5.17.9 #180		
			[ 4070.574903] Hardware name: Intel Corporation NUC7i5BNK/NUC7i5BN B, BIOS BNKBL357.86A.0052.2 017.0918.1346 09/18/2017		
			[ 4070.574907] RIP: 0010:oa_configure_all_c ontexts.isra.0+0x222/0 x350 [i915]		
			[ 4070.574982] Code: 08 e8 32 6e 10 e1 4d 8b 6d 50 b8 ff ff ff ff 49 83 ed 50 f0 41 0f c1 04 24 83 f8 01 0f 84 e3 00 00 00 85 c0 0f 8e fa 00 00 00 <49> 8b 45 50 48 8d 70 b0 49 8d 45 50 48 39 44 24 10 0f 85 34 fe ff		
			[ 4070.574990] RSP: 0018:ffffc90002077b78 EFLAGS: 00010202		
			[ 4070.574995] RAX: 00000000000000002 RBX:		

0-1

1-2

2-33-44-5Page 883 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000002 RCX: 000000000000000000		
			[ 4070.575000] RDX: 000000000000000001 RSI: ffffc90002077b20 RDI: ffff88810ddc7c68		
			[ 4070.575004] RBP: 000000000000000001 R08: ffff888103242648 R09: ffffffffffffff		
			[ 4070.575008] R10: ffffffff82c50bc0 R11: 0000000000025c80 R12: ffff888101bf1860		
			[ 4070.575012] R13: dead000000000000000 R14: ffffc90002077c04 R15: ffff88810be5cabc		
			[ 4070.575016] FS: 00007f1ed50c0780(00 00) GS:ffff888885ec80000(0 000) knlGS:0000000000000 000		
			[ 4070.575021] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			[ 4070.575025] CR2: 00007f1ed5590280 CR3: 000000010ef6f005 CR4: 00000000003706e0		
			[ 4070.575029] Call Trace:		
			[ 4070.575033] <task></task>		

0-1

1-2

**2-3** 3-4 4-5 Page **884** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 4070.575037] lrc_configure_all_contex ts+0x13e/0x150 [i915]		
			[ 4070.575103] gen8_enable_metric_set +0x4d/0x90 [i915]		
			[ 4070.575164] i915_perf_open_ioctl+0 xbc0/0x1500 [i915]		
			[ 4070.575224] ? asm_common_interrupt +0x1e/0x40		
			[ 4070.575232] ? i915_oa_init_reg_state+ 0x110/0x110 [i915]		
			[ 4070.575290] drm_ioctl_kernel+0x85 /0x110		
			[ 4070.575296] ? update_load_avg+0x5f/ 0x5e0		
			[ 4070.575302] drm_ioctl+0x1d3/0x37 0		
			[ 4070.575307] ? i915_oa_init_reg_state+ 0x110/0x110 [i915]		
			[ 4070.575382] ? gen8_gt_irq_handler+0x 46/0x130 [i915]		
			[ 4070.575445] x64_sys_ioctl+0x3c4/ 0x8d0		
			[ 4070.575451] ? do_softirq+0xaa/0x1d 2		
			[ 4070.575456] do_syscall_64+0x35/0x 80		

0-1

1-2

3-4 4-5 2-3

6-7 8-9 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 4070.575461] entry_SYSCALL_64_afte r_hwframe+0x44/0xae		
			[ 4070.575467] RIP: 0033:0x7f1ed5c10397		
			[ 4070.575471] Code: 3c 1c e8 1c ff ff ff 85 c0 79 87 49 c7 c4 ff ff ff ff 5b 5d 4c 89 e0 41 5c c3 66 0f 1f 84 00 00 00 00 00 b8 10 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d a9 da 0d 00 f7 d8 64 89 01 48		
			[ 4070.575478] RSP: 002b:00007ffd65c8d7a 8 EFLAGS: 00000246 ORIG_RAX: 000000000000010		
			[ 4070.575484] RAX: fffffffffffffffda RBX: 00000000000000006 RCX: 00007f1ed5c10397		
			[ 4070.575488] RDX: 00007ffd65c8d7c0 RSI: 0000000040106476 RDI: 0000000000000000006		
			[ 4070.575492] RBP: 00005620972f9c60 R08: 0000000000000000 R09: 0000000000000000		
			[ 4070.575496] R10: 0000000000000000 R11: 0000000000000		

0-1

1-2

**2-3** 3-4 4-5 Page **886** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 4070.575500] R13: 0000000000000000 R14: 000000000000000000000 R15: 00007ffd65c8d7c0		
			[ 4070.575505] 		
			[ 4070.575507] Modules linked in: nls_ascii(E) nls_cp437(E) vfat(E) fat(E) i915(E) x86_pkg_temp_thermal( E) intel_powerclamp(E) crct10dif_pclmul(E) crc32_pclmul(E) crc32_pclmul(E) crc32c_intel(E) aesni_intel(E) crypto_simd(E) intel_gtt(E) cryptd(E) ttm(E) rapl(E) intel_cstate(E) drm_kms_helper(E) cfbfillrect(E) syscopyarea(E) cfbimgblt(E) intel_uncore(E) sysfillrect(E) mei_me(E) sysimgblt(E) i2c_i801(E) fb_sys_fops(E) mei(E) intel_pch_thermal(E) i2c_smbus truncated		
			CVE ID : CVE-2022- 48662		
N/A	28-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/016b150 992eebc32c4 a18f783cf2bb	O-LIN-LINU- 030524/899

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/slub: fix to return errno if kmalloc() fails	6e2545a3d9, https://git.ke rnel.org/stabl	
			In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to	e/c/02bcd95 1aa3c2cea95f b241c20802e 9501940296,	
			out-of-memory, if it fails, return errno correctly rather than	https://git.ke rnel.org/stabl e/c/2d6e55e	
			triggering panic via BUG_ON();	0c03804e1e2 27b80a5746e 086d6c6696c	
			kernel BUG at mm/slub.c:5893!		
			Internal error: Oops - BUG: 0 [#1] PREEMPT SMP		
			Call trace:		
			sysfs_slab_add+0x258/ 0x260 mm/slub.c:5973		
			kmem_cache_create+ 0x60/0x118 mm/slub.c:4899		
			create_cache mm/slab_common.c:22 9 [inline]		
			kmem_cache_create_use rcopy+0x19c/0x31c mm/slab_common.c:33 5		
			kmem_cache_create+0x 1c/0x28 mm/slab_common.c:39 0		

0-1

1-2

2-3 3-4 4-5 Page 888 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f2fs_kmem_cache_creat e fs/f2fs/f2fs.h:2766 [inline]		
			f2fs_init_xattr_caches+0 x78/0xb4 fs/f2fs/xattr.c:808		
			f2fs_fill_super+0x1050/ 0x1e0c fs/f2fs/super.c:4149		
			mount_bdev+0x1b8/0x 210 fs/super.c:1400		
			f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512		
			legacy_get_tree+0x30/0 x74 fs/fs_context.c:610		
			vfs_get_tree+0x40/0x1 40 fs/super.c:1530		
			do_new_mount+0x1dc/ 0x4e4 fs/namespace.c:3040		
			path_mount+0x358/0x 914 fs/namespace.c:3370		
			do_mount fs/namespace.c:3383 [inline]		
			do_sys_mount fs/namespace.c:3591 [inline]		
			se_sys_mount fs/namespace.c:3568 [inline]		

0-1

1-2

**2-3** 3-4 4-5 Page **889** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_arm64_sys_mount+0x 2f8/0x408 fs/namespace.c:3568 <b>CVE ID : CVE-2022-</b> <b>48659</b>		
N/A	28-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: Set lineevent_state::irq after IRQ register successfully When running gpio test on nxp-ls1028 platform with below command gpiomonnum- events=3rising-edge gpiochip1 25 There will be a warning trace as below: Call trace: free_irq+0x204/0x360 lineevent_free+0x64/0x 70 gpio_ioctl+0x598/0x6a 0 arm64_sys_ioctl+0xb4 /0x100 invoke_syscall+0x5c/0x 130	https://git.ke rnel.org/stabl e/c/657803b 918e097e47d 99d1489da83 a603c36bcdd, https://git.ke rnel.org/stabl e/c/69bef19d 6b9700e9628 5f4b4e28691 cda3dcd0d1, https://git.ke rnel.org/stabl e/c/97da736c d11ae73bdf2f 5e21e24446b 8349e0168	O-LIN-LINU- 030524/900
			el0t_64_sync+0x1a0/0x 1a4		

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID		Pato	:h	NCII	PC ID
			The reason of this issu is that calling request_threaded_irq(					
			function failed, and then lineevent_free() i invoked to release	is				
			the resource. Since the lineevent_state::irq wa already set, so					
			the subsequent invocation of free_irq( would trigger the abov					
			warning call trace. To fix this issue, set the lineevent_state::irq					
			after the IRQ register successfully.					
			CVE ID : CVE-2022- 48660					
			In the Linux kernel, the following vulnerability has been resolved:		https:/// rnel.org/ e/c/027 091ccfb2	/stabl 43c4		
Improper Resource Shutdown	28-Apr-2024	5.5	gpio: mockup: Fix potential resource leakage when register chip	a	cdbbe3f 52d5d12 https:// rnel.org, e/c/41f8 3c44442	44b1 2933, git.ke /stabl 35703	0-LIN- 03052	
or Release			If creation of software node fails, the locally allocated string	•	591fda8d986 e7c9e42872, https://git.ke	872, git.ke		
			array is left unfreed. Free it on error path.		rnel.org, e/c/9b2 e058faat	6723		
			CVE ID : CVE-2022- 48661		32fb4aa 849d582	16d6		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.79								
Concurrent Execution using	17-Apr-2024	4.7	In the Linux kernel, the following vulnerability has been resolved:		https:// rnel.org, e/c/653	/stabl	O-LIN- 03052	
CVSS Scoring S	Scale 0-1	1-2 2	<b>-3</b> 3-4 4-5 5	5-6	6-7	7-8	8-9	9-10
0100 000 mg 0		2				, 0	0.5	0 10

Page 891 of 1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchroniz ation			netfilter: ipset: fix performance regression in swap operation	d9995d7d5f4 97c665b3218 75a626161c, https://git.ke rnel.org/stabl e/c/970709a	
('Race Condition')			The patch "netfilter: ipset: fix race condition between swap/destroy and kernel side add/del/test", commit	67696b100a5 7b33af1a3d7 5fc34b747eb, https://git.ke rnel.org/stabl	
			28628fa9 fixes a race condition.	e/c/97f7cf1cd 80eeed3b7c8 08b7c124632	
			But the synchronize_rcu() added to the swap function unnecessarily slows	95c751001	
			it down: it can safely be moved to destroy and use call_rcu() instead.		
			Eric Dumazet pointed out that simply calling the destroy functions as		
			rcu callback does not work: sets with timeout use garbage collectors		
			which need cancelling at destroy which can wait. Therefore the destroy		
			functions are split into two: cancelling garbage collectors safely at		
			executing the command received by netlink and moving the remaining		
			part only into the rcu callback.		

0-1

1-2

2-33-44-5Page 892 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2024- 26910					
Affected Vers	Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.80							
	sion(s): From (i	ncluding)	In the Linux kernel, the following vulnerability has been resolved: pmdomain: mediatek: fix race conditions with genpd If the power domains are registered first with genpd and *after that* the driver attempts to power them on in the	.80 https://git.ke rnel.org/stabl e/c/339ddc9 83bc1622341				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	using Shared Resource with 17-Apr-2024 Improper Synchroniz ation ('Race	4.7	probe sequence, then it is possible that a race condition occurs if genpd tries to power them on in the same time. The same is valid for powering them off before unregistering them	d95f244c361c da3da3a4ff, https://git.ke rnel.org/stabl e/c/3cd1d92e e1dbf3e8f988 767eb75f262 07397792b, https://git.ke rnel.org/stabl e/c/475426a	O-LIN-LINU- 030524/903			
			from genpd.	d1ae0bfdfd8f 160ed975090				
					Attempt to fix race conditions by first removing the domains from genpd	3799392438		
					and *after that* powering down domains.			
		Also first power up the domains and *after that* register them						
			to genpd.					

0-1

1-2

2-33-44-5Page 893 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 52645		
Affected Ver	sion(s): From (i	ncluding)	5.16 Up to (excluding) 6.1	.83	
Affected Ver	sion(s): From (i	ncluding) 7.8	<ul> <li>5.16 Up to (excluding) 6.1</li> <li>In the Linux kernel, the following vulnerability has been resolved:</li> <li>net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv()</li> <li>Apply the same fix than ones found in :</li> <li>8d975c15c0cd ("ip6_tunnel: make sure to pull inner header inip6_tnl_rcv()")</li> <li>1ca1ba465e55 ("geneve: make sure to pull inner header in geneve_rx()")</li> <li>We have to save skb-&gt;network_header in a temporary variable in order to be able to recompute the network_header pointer after a pskb_inet_may_pull() call.</li> <li>pskb_inet_may_pull() makes sure the needed headers are in skb-&gt;head.</li> </ul>	.83 https://git.ke rnel.org/stabl e/c/5c03387 021cfa3336b 97e0dcba380 29917a8af2a, https://git.ke rnel.org/stabl e/c/60044ab 84836359534 bd7153b92e9 c1584140e4a, https://git.ke rnel.org/stabl e/c/77fd5294 ea09b21f677 2ac954a121b 87323cec80	O-LIN-LINU- 030524/904

0-1

1-2

**2-3** 3-4 4-5 Page **894** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syzbot reported:		
			BUG: KMSAN: uninit- value in INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			BUG: KMSAN: uninit- value in INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			BUG: KMSAN: uninit- value in IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			BUG: KMSAN: uninit- value in ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		

0-1

1-2

2-33-44-5Page 895 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ipgre_rcv+0x9bc/0xb c0 net/ipv4/ip_gre.c:389		
			ipgre_rcv net/ipv4/ip_gre.c:411 [inline]		
			gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447		
			gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c: 163		
			ip_protocol_deliver_rcu +0x264/0x1300 net/ipv4/ip_input.c:205		
			ip_local_deliver_finish+ 0x2b8/0x440 net/ipv4/ip_input.c:233		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_local_deliver+0x21f/ 0x490 net/ipv4/ip_input.c:254		
			dst_input include/net/dst.h:461 [inline]		
			ip_rcv_finish net/ipv4/ip_input.c:449 [inline]		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569		
			netif_receive_skb_one		

0-1

1-2

2-3 3-4 4-5 Page **896** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_core net/core/dev.c:5534 [inline]		
			netif_receive_skb+0x1 a6/0x5a0 net/core/dev.c:5648		
			netif_receive_skb_intern al net/core/dev.c:5734 [inline]		
			netif_receive_skb+0x58 /0x660 net/core/dev.c:5793		
			tun_rx_batched+0x3ee/ 0x980 drivers/net/tun.c:1556		
			tun_get_user+0x53b9/0 x66e0 drivers/net/tun.c:2009		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			Uninit was created at:		
			alloc_pages+0x9a6/0x e00 mm/page_alloc.c:4590		
			alloc_pages_mpol+0x62 b/0x9d0 mm/mempolicy.c:2133		
			alloc_pages+0x1be/0x1 e0 mm/mempolicy.c:2204		
			skb_page_frag_refill+0x 2bf/0x7c0 net/core/sock.c:2909		

0-1

1-2

**2-3** 3-4 4-5 Page **898** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tun_build_skb drivers/net/tun.c:1686 [inline]		
			tun_get_user+0xe0a/0x 66e0 drivers/net/tun.c:1826		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0		

0-1

1-2

5-6

6-7

 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			CVE ID : CVE-2024- 26882		
			In the Linux kernel, the following vulnerability has been resolved:		
			bpf: Fix stackmap overflow check on 32- bit arches		
			The stackmap code relies on roundup_pow_of_two() to compute the number	https://git.ke rnel.org/stabl e/c/0971126 c8164abe200 4b8536b4969	
Improper Restriction of			of hash buckets, and contains an overflow check by checking if the	0a0d6005b0a, https://git.ke rnel.org/stabl	
Operations within the Bounds of a Memory	17-Apr-2024	7.8	resulting value is 0. However, on 32-bit arches, the roundup code itself	e/c/1564100 7df0f0d35fa2 8742b25c2a7 db9dcd6895,	O-LIN-LINU- 030524/905
Buffer			can overflow by doing a 32-bit left-shift of an unsigned long value,	https://git.ke rnel.org/stabl e/c/21e5fa46 88e1a4d3db6	
			which is undefined behaviour, so it is not guaranteed to truncate	b72216231b2 4232f75c1d	
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code.		

0-1

1-2

**2-3** 3-4 4-5 Page **900** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The commit in the fixes tag actually attempted to fix this, but the fix did not account for the UB, so the fix only works on CPUs where an overflow does result in a neat truncation to zero, which is not guaranteed. Checking the value before rounding does not have this problem. <b>CVE ID : CVE-2024-</b> <b>26883</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix hashtab overflow check on 32- bit arches The hashtab code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit arches, the roundup code itself	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d 92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6 5f07b1132c1 979d73f014a e6e04de55d, https://git.ke rnel.org/stabl e/c/64f00b4d f0597590b19 9b62a37a165 473bf658a6	O-LIN-LINU- 030524/906

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code. So apply the same		
			fix to hashtab, by moving the overflow check to before the roundup.		
			CVE ID : CVE-2024- 26884		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl	
Improper Restriction			bpf: Fix DEVMAP_HASH overflow check on 32- bit arches	e/c/22079b3 a423382335f 47d9ed32114 e6c9fe88d7c, https://git.ke	
of Operations within the Bounds of a Memory	17-Apr-2024	7.8	The devmap code allocates a number hash buckets equal to the next power	rnel.org/stabl e/c/225da02 acdc97af01b6 bc6ce1a3e53 62bf01d3fb,	O-LIN-LINU- 030524/907
Buffer			of two of the max_entries value provided when creating the map. When	https://git.ke rnel.org/stabl e/c/250051ac c21f9d4c5c59 5e4fcb55986e	
			rounding up to the next power of two, the 32-bit variable storing the	a08c4691	

0-1

1-2

2-33-44-5Page 902 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			number of buckets can overflow, and the code checks for overflow by		
			checking if the truncated 32-bit value is equal to 0. However, on 32-bit		
			arches the rounding up itself can overflow mid- way through, because it		
			ends up doing a left- shift of 32 bits on an unsigned long value. If the		
			size of an unsigned long is four bytes, this is undefined behaviour, so		
			there is no guarantee that we'll end up with a nice and tidy 0-value at		
			the end.		
			Syzbot managed to turn this into a crash on arm32 by creating a		
			DEVMAP_HASH with max_entries > 0x80000000 and then trying to update it.		
			Fix this by moving the overflow check to before the rounding up		
			operation. CVE ID : CVE-2024- 26885		
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/079cba4f 4e307c69878 226fdf5228c2	O-LIN-LINU- 030524/908

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts	0aa1c969c, https://git.ke rnel.org/stabl e/c/1a54aa50	
			This patch is against CVE-2023-6270. The description of cve is:	6b3b2f31496 731039e4977 8f54eee881, https://git.ke	
			A flaw was found in the ATA over Ethernet (AoE) driver in the Linux	rnel.org/stabl e/c/74ca3ef6 8d2f449bc84 8c0a814cefc4 87bf755fa	
			kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on		
			`struct net_device`, and a use-after-free can be triggered by racing		
			between the free on the struct and the access through the `skbtxq`		
			global queue. This could lead to a denial of service condition or		
			potential code execution.		
			In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial		
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in		

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		
			This patch removed the dev_put(ifp) in the success path in		
			aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx().		
			CVE ID : CVE-2024- 26898		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/185fa070 00e0a81d54cf	
			RDMA/mlx5: Fix fortify source warning while accessing Eth segment	8c05414cebff 14469a5c, https://git.ke rnel.org/stabl	
N/A	17-Apr-2024	7.8	[ cut here ]	e/c/4d5e86a 56615cc387d 21c629f9af8f	O-LIN-LINU- 030524/909
			memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start"	b0e958d350, https://git.ke rnel.org/stabl e/c/60ba938	
			at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive	a8bc8c90e72 4c75f98e932f 9fb7ae1b9d	

0-1

1-2

2-33-44-5Page 905 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rs/infiniband/hw/mlx5		
			/wr.c:131 (size 2)		
			WARNING: CPU: 0 PID:		
			293779 at		
			/var/lib/dkms/mlnx-		
			ofed-		
			kernel/5.8/build/drive		
			rs/infiniband/hw/mlx5		
			/wr.c:131		
			mlx5_ib_post_send+0x1		
			91b/0x1a60 [mlx5_ib]		
			Modules linked in:		
			8021q garp mrp stp llc		
			rdma_ucm(OE)		
			rdma_cm(OE)		
			iw_cm(OE) ib_ipoib(OE)		
			ib_cm(OE) ib_umad(OE)		
			mlx5_ib(OE)		
			ib_uverbs(OE)		
			ib_core(OE)		
			mlx5_core(OE)		
			pci_hyperv_intf mlxdevm(OE)		
			mlx_compat(OE) tls		
			mlxfw(OE) psample		
			nft_fib_inet nft_fib_ipv4		
			nft_fib_ipv6 nft_fib		
			nft_reject_inet		
			nf_reject_ipv4		
			nf_reject_ipv6 nft_reject		
			nft_ct nft_chain_nat		
			nf_nat nf_conntrack		
			nf_defrag_ipv6		
			nf_defrag_ipv4 ip_set		
			nf_tables libcrc32c		
			nfnetlink		
			mst_pciconf(OE)		
			knem(OE) vfio_pci		
			vfio_pci_core		
			vfio_iommu_type1 vfio		
			iommufd irqbypass cuse nfsv3 nfs fscache		
			netfs xfrm_user		
			וופעס אוו ווו_עספו		

0-1

1-2

2-3 3-4 4-5 Page **906** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xfrm_algo ipmi_devintf ipmi_msghandler binfmt_misc crct10dif_pclmul crc32_pclmul polyval_clmulni polyval_generic ghash_clmulni_intel sha512_ssse3 snd_pcsp aesni_intel crypto_simd cryptd snd_pcm snd_timer joydev snd		
			soundcore input_leds serio_raw evbug nfsd auth_rpcgss nfs_acl lockd grace sch_fq_codel sunrpc drm efi_pstore ip_tables x_tables autofs4 psmouse virtio_net net_failover failover floppy		
			[last unloaded: mlx_compat(OE)] CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2.0-32-generic #32~22.04.1-Ubuntu Hardware name: Red		
			Hat KVM, BIOS 0.5.1 01/01/2011 RIP: 0010:mlx5_ib_post_sen d+0x191b/0x1a60 [mlx5_ib] Code: 0c 01 00 a8 01		
			75 25 48 8b 75 a0 b9 02 00 00 00 48 c7 c2 10 5b fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01 e8 95 4d 93 da <0f> 0b 44 8b 4d b0 4c 8b 45 c8		

0-1

1-2

2-33-44-5Page 907 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			48 8b 4d c0 e9 49 fb ff ff 41 0f b7		
			RSP: 0018:ffffb5b48478b570 EFLAGS: 00010046		
			RAX: 000000000000000000 RBX: 00000000000000001 RCX: 000000000000000000000000000000000000		
			RDX: 000000000000000000 RSI: 000000000000000000000 RDI: 000000000000000000000000000000000000		
			RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000		
			R10: 0000000000000000 R11: 0000000000000		
			R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80		
			FS: 00007fc03b444c80(00 00) GS:ffff963a3dc00000(0 000) knlGS:0000000000000 000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CR2: 0000556f46bdf000 CR3: 000000006ac6003 CR4: 0000000003706f0		
			DR0: 00000000000000000 DR1: 00000000000000000 DR2: 000000000000000000000000000000000000		
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		
			<task></task>		
			? show_regs+0x72/0x90		
			? mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?_warn+0x8d/0x160		
			? mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			? report_bug+0x1bb/0x1 d0		
			? handle_bug+0x46/0x90		
			? exc_invalid_op+0x19/0 x80		
			?		
			i asm_exc_invalid_op+0x 1b/0x20		

0-1

1-2

**2-3** 3-4 4-5 Page **909** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			mlx5_ib_post_send_nod rain+0xb/0x20 [mlx5_ib]		
			ipoib_send+0x2ec/0x77 0 [ib_ipoib]		
			ipoib_start_xmit+0x5a0 /0x770 [ib_ipoib]		
			dev_hard_start_xmit+0x 8e/0x1e0 ?		
			validate_xmit_skb_list+ 0x4d/0x80		
			sch_direct_xmit+0x116 /0x3a0		
			dev_xmit_skb+0x1fd/ 0x580		
			dev_queue_xmit+0x28 4/0x6b0 ?		
			_raw_spin_unlock_irq+0 xe/0x50 ?		
			flush_work.isra.0+0x2 0d/0x370 ?		
			push_pseudo_header+0 x17/0x40 [ib_ipoib]		
			neigh_connected_outpu t+0xcd/0x110		

0-1

1-2

2-33-44-5Page 910 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_finish_output2+0x17 9/0x480 ? smp_call_single_queue +0x61/0xa0		
			ip_finish_output+0xc3 /0x190		
			ip_finish_output+0x2e/ 0xf0		
			ip_output+0x78/0x110 ? pfx_ip_finish_output+		
			0x10/0x10 ip_local_out+0x64/0x7 0		
			ip_queue_xmit+0x18a /0x460		
			ip_queue_xmit+0x15/0 x30		
			tcp_transmit_skb+0x9 14/0x9c0		
			tcp_write_xmit+0x334/ 0x8d0		
			tcp_push_one+0x3c/0x 60		
			tcp_sendmsg_locked+0x 2e1/0xac0		

0-1

1-2

5-6

6-7

 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_sendmsg+0x2d/0x5 0		
			inet_sendmsg+0x43/0x 90		
			sock_sendmsg+0x68/0x 80		
			sock_write_iter+0x93/0 x100		
			vfs_write+0x326/0x3c0		
			ksys_write+0xbd/0xf0		
			?		
			do_syscall_64+0x69/0x 90		
			x64_sys_write+0x19/ 0x30		
			do_syscall_		
			truncated		
			CVE ID : CVE-2024- 26907		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/0fbcf236 6ba9888cf02e da23e35fde7f	
NULL Pointer Dereferenc e	17-Apr-2024	5.5	net: hns3: fix kernel crash when 1588 is received on HIP08 devices	7fcc07c3, https://git.ke rnel.org/stabl e/c/11b9983 60d96f6c76f0 4a95f54b49f2	O-LIN-LINU- 030524/910
			The HIP08 devices does not register the ptp devices, so the	4d3c858e4, https://git.ke rnel.org/stabl e/c/23ec1cec	

0-1

1-2

2-33-44-5Page 912 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hdev->ptp is NULL, but the hardware can receive 1588 messages,	24293f9799c 725941677d4 e167997265	
			and set the HNS3_RXD_TS_VLD_B bit, so, if match this case, the		
			access of hdev->ptp- >flags will cause a kernel crash:		
			[ 5888.946472] Unable to handle kernel NULL pointer dereference at virtual address 000000000000018		
			[ 5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 00000000000018		
			 [ 5889.266118] pc : hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.272612] lr : hclge_ptp_get_rx_hwts+ 0x34/0x170 [hclge]		
			[ 5889.279101] sp : ffff800012c3bc50		
			[ 5889.283516] x29: ffff800012c3bc50 x28: ffff2040002be040		
			[ 5889.289927] x27: ffff800009116484 x26: 0000000080007500		
			[ 5889.296333] x25: 00000000000000000 x24: ffff204001c6f000		

0-1

1-2

2-33-44-5Page 913 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.302738] x23: ffff204144f53c00 x22: 00000000000000000		
			[ 5889.309134] x21: 00000000000000000 x20: ffff204004220080		
			[ 5889.315520] x19: ffff204144f53c00 x18: 00000000000000000		
			[ 5889.321897] x17: 00000000000000000 x16:		
			0000000000000000 [ 5889.328263] x15: 0000004000140ec8 x14: 00000000000000000000000		
			[ 5889.334617] x13: 00000000000000000 x12: 00000000010011df		
			[ 5889.340965] x11: bbfeff4d22000000 x10: 00000000000000000		
			[ 5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d		
			[ 5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480		
			[ 5889.359959] x5 : 0000000000000000 x4 : 00000000000000000		
			[ 5889.366271] x3 : 0000000000000000 x2 : 00000000000000000		
			[ 5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		

0-1

1-2

2-33-44-5Page 914 of 1051

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.378857] Call trace:		
			[ 5889.382285] hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.388304] hns3_handle_bdinfo+0x 324/0x410 [hns3]		
			[ 5889.394055] hns3_handle_rx_bd+0x6 0/0x150 [hns3]		
			[ 5889.399624] hns3_clean_rx_ring+0x8 4/0x170 [hns3]		
			[ 5889.405270] hns3_nic_common_poll +0xa8/0x220 [hns3]		
			[ 5889.411084] napi_poll+0xcc/0x264		
			[ 5889.415329] net_rx_action+0xd4/0x 21c		
			[ 5889.419911] do_softirq+0x130/0x 358		
			[ 5889.424484] irq_exit+0x134/0x154		
			[ 5889.428700] handle_domain_irq+0 x88/0xf0		
			[ 5889.433684] gic_handle_irq+0x78/0 x2c0		
			[ 5889.438319] el1_irq+0xb8/0x140		
			[ 5889.442354] arch_cpu_idle+0x18/0x 40		

0-1

1-2

2-33-44-5Page 915 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.446816] default_idle_call+0x5c/ 0x1c0		
			[ 5889.451714] cpuidle_idle_call+0x174 /0x1b0		
			[ 5889.456692] do_idle+0xc8/0x160		
			[ 5889.460717] cpu_startup_entry+0x3 0/0xfc		
			[ 5889.465523] secondary_start_kernel +0x158/0x1ec		
			[ 5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80)		
			[ 5889.477950] SMP: stopping secondary CPUs		
			[ 5890.514626] SMP: failed to stop secondary CPUs 0-69,71-95		
			[ 5890.522951] Starting crashdump kernel		
			CVE ID : CVE-2024- 26881		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/3948abaa 4e2be938ccdf c289385a273	
Use of Uninitialize d Resource	17-Apr-2024	5.5	do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak	42fb13d43, https://git.ke rnel.org/stabl e/c/423b6bdf	0-LIN-LINU- 030524/911
			syzbot identified a kernel information leak vulnerability in	19bbc5e1f7e7 46104509991 7378f7e71, https://git.ke	

0-1

1-2

2-33-44-5Page 916 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_handle () and issued the following report [1].	rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228	
			[1]	a68d8a7c1	
			"BUG: KMSAN: kernel- infoleak in instrument_copy_to_use		
			r		
			include/linux/instrume nted.h:114 [inline]		
			BUG: KMSAN: kernel- infoleak in		
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40		
			instrument_copy_to_use r		
			include/linux/instrume nted.h:114 [inline]		
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40		
			copy_to_user include/linux/uaccess.h :191 [inline]		
			do_sys_name_to_handle fs/fhandle.c:73 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		

0-1

1-2

2-33-44-5Page 917 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517 do_kmalloc_node		
			mm/slab_common.c:10 06 [inline]		
			_kmalloc+0x121/0x3c 0		
			mm/slab_common.c:10 20		
			kmalloc include/linux/slab.h:60 4 [inline]		
			do_sys_name_to_handle fs/fhandle.c:39 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			 Bytes 18-19 of 20 are uninitialized Memory access of size 20 starts at ffff888128a46380 Data copied to user address 000000020000240" Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to solve the problem.		
NULL Pointer Dereferenc e	17-Apr-2024	5.5	CVE ID : CVE-2024- 26901 In the Linux kernel, the following vulnerability has been resolved: Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security During our fuzz testing of the connection and disconnection process at the RFCOMM layer, we discovered this bug. By comparing the packets from a normal connection and disconnection process with the testcase that triggered a KASAN report. We analyzed the	https://git.ke rnel.org/stabl e/c/2535b84 8fa0f42ddff3e 5255cf5e742c 9b77bb26, https://git.ke rnel.org/stabl e/c/369f419c 097e82407dd 429a202cde9 a73d3ae29b, https://git.ke rnel.org/stabl e/c/3ead59ba fad05f2967ae 2438c0528d5 3244cfde5	O-LIN-LINU- 030524/912

0-1

1-2

2-33-44-5Page 919 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause of this bug as follows:		
			1. In the packets captured during a normal connection, the host sends a		
			`Read Encryption Key Size` type of `HCI_CMD` packet		
			(Command Opcode: 0x1408) to the controller to inquire the length of		
			encryption key.After receiving this packet, the controller immediately		
			replies with a Command Completepacket (Event Code: 0x0e) to return the		
			Encryption Key Size.		
			2. In our fuzz test case, the timing of the controller's response to this		
			packet was delayed to an unexpected point: after the RFCOMM and L2CAP		
			layers had disconnected but before the HCI layer had disconnected.		
			3. After receiving the Encryption Key Size		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Response at the time described		
			in point 2, the host still called the rfcomm_check_security function.		
			However, by this time `struct l2cap_conn *conn = l2cap_pi(sk)- >chan->conn;`		
			had already been released, and when the function executed		
			`return hci_conn_security(conn ->hcon, d->sec_level, auth_type, d->out);`,		
			specifically when accessing `conn->hcon`, a null-ptr-deref error occurred.		
			To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling		
			rfcomm_recv_frame in rfcomm_process_rx.		
			CVE ID : CVE-2024- 26903		
Affected Ver	sion(s): From (i	ncluding)	5.3 Up to (excluding) 6.7.1	1	
Missing Release of Memory	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/4c1021ce 46fc2fb6115f 7e79d353941	O-LIN-LINU-
after Effective Lifetime			md: fix kmemleak of rdev->serial	e6dcad366, https://git.ke rnel.org/stabl e/c/6cf35065	030524/913

0-1

1-2

2-33-44-5Page 921 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If kobject_add() is fail in bind_rdev_to_array(), 'rdev->serial' will be	8736681b9d6 b0b6e58c5c7 6b235bb4c4,	
			alloc not be freed, and kmemleak occurs.	https://git.ke rnel.org/stabl e/c/6d32c83 2a88513f65c	
			unreferenced object 0xffff88815a350000 (size 49152):	2c2c9c75954 ee8b387adea	
			comm "mdadm", pid 789, jiffies 4294716910		
			hex dump (first 32 bytes):		
			00 00 00 00 00 00 00 00 00 00 00 00 00 0		
			00 00 00 00 00 00 00 00 00 00 00 00 00 0		
			backtrace (crc f773277a):		
			[<0000000058b0a453> 1		
			kmemleak_alloc+0x61/ 0xe0		
			[<00000000366adf14> ]		
			kmalloc_large_node+0 x15e/0x270		
			[<000000002e82961b> ]		
			kmalloc_node.cold+0x 11/0x7f		
			[<00000000f206d60a> ]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kvmalloc_node+0x74/0 x150		
			[<0000000034bf3363> ]		
			rdev_init_serial+0x67/0 x170		
			[<0000000010e08fe9>] mddev_create_serial_po ol+0x62/0x220		
			[<00000000c3837bf0>] bind_rdev_to_array+0x 2af/0x630		
			[<0000000073c28560>		
			nd_add_new_disk+0x4 00/0x9f0		
			[<00000000770e30ff>] md_ioctl+0x15bf/0x1c1 0		
			[<000000006cfab718>] blkdev_ioctl+0x191/0x 3f0		
			[<0000000085086a11> ] vfs_ioctl+0x22/0x60		
			[<0000000018b656fe>		
			] x64_sys_ioctl+0xba/0 xe0		
			[<00000000e54e675e> ]		
			do_syscall_64+0x71/0x 150		

0-1

1-2

2-33-44-5Page 923 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<00000008b0ad622> ] entry_SYSCALL_64_afte r_hwframe+0x6c/0x74 CVE ID : CVE-2024- 26900		
Affected Vers	sion(s): From (i	ncluding)	5.4 Up to (excluding) 5.10	.214	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix DEVMAP_HASH overflow check on 32- bit arches The devmap code allocates a number hash buckets equal to the next power of two of the max_entries value provided when creating the map. When rounding up to the next power of two, the 32-bit variable storing the number of buckets can overflow, and the code checks for overflow by checking if the truncated 32-bit value is equal to 0. However, on 32-bit arches the rounding up itself can overflow mid- way through, because it	https://git.ke rnel.org/stabl e/c/22079b3 a423382335f 47d9ed32114 e6c9fe88d7c, https://git.ke rnel.org/stabl e/c/225da02 acdc97af01b6 bc6ce1a3e53 62bf01d3fb, https://git.ke rnel.org/stabl e/c/250051ac c21f9d4c5c59 5e4fcb55986e a08c4691	O-LIN-LINU- 030524/914
			ends up doing a left- shift of 32 bits on an		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unsigned long value. If the		
			size of an unsigned long is four bytes, this is undefined behaviour, so		
			there is no guarantee that we'll end up with a nice and tidy 0-value at		
			the end.		
			Syzbot managed to turn this into a crash on arm32 by creating a		
			DEVMAP_HASH with max_entries > 0x80000000 and then trying to update it.		
			Fix this by moving the overflow check to before the rounding up		
			operation.		
			CVE ID : CVE-2024- 26885		
Affected Ver	sion(s): From (i	ncluding)	5.5 Up to (excluding) 5.10	.146	
		28-Apr-2024 5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/016b150 992eebc32c4 a18f783cf2bb	
N/A 28-Apr-20	28-Apr-2024		mm/slub: fix to return errno if kmalloc() fails	6e2545a3d9, https://git.ke rnel.org/stabl e/c/02bcd95	O-LIN-LINU- 030524/915
			In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to	1aa3c2cea95f b241c20802e 9501940296,	
			out-of-memory, if it fails, return errno correctly rather than	https://git.ke rnel.org/stabl e/c/2d6e55e 0c03804e1e2	

0-1

1-2

2-33-44-5Page 925 of 1051

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggering panic via BUG_ON();	27b80a5746e 086d6c6696c	
			kernel BUG at mm/slub.c:5893!		
			Internal error: Oops - BUG: 0 [#1] PREEMPT SMP		
			Call trace:		
			sysfs_slab_add+0x258/ 0x260 mm/slub.c:5973		
			kmem_cache_create+ 0x60/0x118 mm/slub.c:4899		
			create_cache mm/slab_common.c:22 9 [inline]		
			kmem_cache_create_use rcopy+0x19c/0x31c mm/slab_common.c:33 5		
			kmem_cache_create+0x 1c/0x28 mm/slab_common.c:39 0		
			f2fs_kmem_cache_creat e fs/f2fs/f2fs.h:2766 [inline]		
			f2fs_init_xattr_caches+0 x78/0xb4 fs/f2fs/xattr.c:808		
			f2fs_fill_super+0x1050/		

0-1

1-2

2-33-44-5Page 926 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x1e0c fs/f2fs/super.c:4149		
			mount_bdev+0x1b8/0x 210 fs/super.c:1400		
			f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512		
			legacy_get_tree+0x30/0 x74 fs/fs_context.c:610		
			vfs_get_tree+0x40/0x1 40 fs/super.c:1530		
			do_new_mount+0x1dc/ 0x4e4 fs/namespace.c:3040		
			path_mount+0x358/0x 914 fs/namespace.c:3370		
			do_mount fs/namespace.c:3383 [inline]		
			do_sys_mount fs/namespace.c:3591 [inline]		
			se_sys_mount fs/namespace.c:3568 [inline]		
			arm64_sys_mount+0x 2f8/0x408 fs/namespace.c:3568		
			CVE ID : CVE-2022- 48659		
Affected Vers	sion(s): From (i	ncluding)	5.5 Up to (excluding) 5.10	.210	

0-1

1-2

3-4 4-5 2-3 Page 927 of 1051

7-8 8-9 9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	:	In the Linux kernel, the following vulnerability has been resolved:			
			netfilter: ipset: fix performance regression in swap operation		
Concurrent Execution using Shared Resource with Improper Synchroniz	on ce 17-Apr-2024 4.7	17-Apr-2024 4.7	and kernel side add/del/test", commit 28628fa9 fixes a race condition.rnel.org/ e/c/653 d9995d7 97c665b 75a6261 https://f rnel.org/ e/c/653 97c665b 75a6261 https://f rnel.org/ e/c/970 67696b1	https://git.ke rnel.org/stabl e/c/653bc5e6 d9995d7d5f4 97c665b3218 75a626161c, https://git.ke rnel.org/stabl e/c/970709a 67696b100a5 7b33af1a3d7 5fc34b747eb,	0-LIN-LINU- 030524/916
ation ('Race Condition')			it down: it can safely be moved to destroy and use call_rcu() instead. Eric Dumazet pointed	https://git.ke rnel.org/stabl e/c/97f7cf1cd 80eeed3b7c8	
			out that simply calling the destroy functions as	08b7c124632 95c751001	
			rcu callback does not work: sets with timeout use garbage collectors		
			which need cancelling at destroy which can wait. Therefore the destroy		
			functions are split into two: cancelling garbage collectors safely at		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executing the command received by netlink and moving the remaining		
			part only into the rcu callback.		
			CVE ID : CVE-2024- 26910		
Affected Ver	sion(s): From (i	ncluding)	5.5 Up to (excluding) 5.10	.214	
			In the Linux kernel, the following vulnerability has been resolved:		
			net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv()	https://git.ke rnel.org/stabl	
			Apply the same fix than ones found in :	e/c/5c03387 021cfa3336b 97e0dcba380 29917a8af2a,	
N/A	17-Apr-2024	7.8	8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in ip6_tnl_rcv()")	https://git.ke rnel.org/stabl e/c/60044ab 84836359534	O-LIN-LINU- 030524/917
			1ca1ba465e55 ("geneve: make sure to pull inner header in geneve_rx()")	bd7153b92e9 c1584140e4a, https://git.ke rnel.org/stabl e/c/77fd5294	
			We have to save skb- >network_header in a temporary variable	ea09b21f677 2ac954a121b 87323cec80	
			in order to be able to recompute the network_header pointer		
			after a pskb_inet_may_pull() call.		

0-1

1-2

2-33-44-5Page 929 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pskb_inet_may_pull() makes sure the needed headers are in skb- >head.		
			syzbot reported: BUG: KMSAN: uninit- value in INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			BUG: KMSAN: uninit- value in INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			BUG: KMSAN: uninit- value in IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			BUG: KMSAN: uninit- value in ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40		
			9 INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		

0-1

1-2

2-33-44-5Page 930 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			ipgre_rcv+0x9bc/0xb c0 net/ipv4/ip_gre.c:389		
			ipgre_rcv net/ipv4/ip_gre.c:411 [inline]		
			gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447		
			gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c: 163		
			ip_protocol_deliver_rcu +0x264/0x1300 net/ipv4/ip_input.c:205		
			ip_local_deliver_finish+ 0x2b8/0x440 net/ipv4/ip_input.c:233		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_local_deliver+0x21f/ 0x490 net/ipv4/ip_input.c:254		
			dst_input include/net/dst.h:461 [inline]		
			ip_rcv_finish net/ipv4/ip_input.c:449 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569		
			netif_receive_skb_one _core net/core/dev.c:5534 [inline]		
			netif_receive_skb+0x1 a6/0x5a0 net/core/dev.c:5648		
			netif_receive_skb_intern al net/core/dev.c:5734 [inline]		
			netif_receive_skb+0x58 /0x660 net/core/dev.c:5793		
			tun_rx_batched+0x3ee/ 0x980 drivers/net/tun.c:1556		
			tun_get_user+0x53b9/0 x66e0 drivers/net/tun.c:2009		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		

0-1

1-2

2-33-44-5Page 932 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			Uninit was created at:		
			alloc_pages+0x9a6/0x e00 mm/page_alloc.c:4590		
			alloc_pages_mpol+0x62 b/0x9d0 mm/mempolicy.c:2133		
			alloc_pages+0x1be/0x1		

0-1

1-2

5-6

6-7

7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e0 mm/mempolicy.c:2204		
			skb_page_frag_refill+0x 2bf/0x7c0 net/core/sock.c:2909		
			tun_build_skb drivers/net/tun.c:1686 [inline]		
			tun_get_user+0xe0a/0x 66e0 drivers/net/tun.c:1826		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		

0-1

1-2

3-4 4-5 2-3

8-9 7-8 9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			CVE ID : CVE-2024- 26882		
			In the Linux kernel, the following vulnerability has been resolved:		
			bpf: Fix stackmap overflow check on 32- bit arches	https://git.ke rnel.org/stabl e/c/0971126	
Improper Restriction of			The stackmap code relies on roundup_pow_of_two() to compute the number	c8164abe200 4b8536b4969 0a0d6005b0a, https://git.ke rnel.org/stabl	
Operations within the Bounds of	17-Apr-2024	7.8	of hash buckets, and contains an overflow check by checking if the	e/c/1564100 7df0f0d35fa2 8742b25c2a7	O-LIN-LINU- 030524/918
a Memory Buffer			resulting value is 0. However, on 32-bit arches, the roundup code itself	db9dcd6895, https://git.ke rnel.org/stabl e/c/21e5fa46	
			can overflow by doing a 32-bit left-shift of an unsigned long value,	88e1a4d3db6 b72216231b2 4232f75c1d	
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on		

0-1

1-2

2-33-44-5Page 935 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the DEVMAP_HASH type, which contains the same		
			check, copied from the hashtab code.		
			The commit in the fixes tag actually attempted to fix this, but the fix		
			did not account for the UB, so the fix only works on CPUs where an		
			overflow does result in a neat truncation to zero, which is not		
			guaranteed. Checking the value before rounding does not have this		
			problem.		
			CVE ID : CVE-2024- 26883		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d	
Improper Restriction of Operations within the Bounds of a Memory Buffer		24 7.8	bpf: Fix hashtab overflow check on 32- bit arches	92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6	O-LIN-LINU-
	17-Apr-2024		The hashtab code relies on roundup_pow_of_two() to compute the number	5f07b1132c1 979d73f014a e6e04de55d, https://git.ke rnel.org/stabl	030524/919
			of hash buckets, and contains an overflow check by checking if the	e/c/64f00b4d f0597590b19 9b62a37a165 473bf658a6	

0-1

1-2

2-33-44-5Page 936 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting value is 0. However, on 32-bit arches, the roundup code itself		
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code. So apply the same		
			fix to hashtab, by moving the overflow check to before the roundup.		
			CVE ID : CVE-2024- 26884		
		17-Apr-2024 7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/079cba4f 4e307c69878	
Use After Free 17-Apr-2024	17-Apr-2024		aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts	226fdf5228c2 0aa1c969c, https://git.ke rnel.org/stabl e/c/1a54aa50	O-LIN-LINU- 030524/920
		This patch is against CVE-2023-6270. The description of cve is:	6b3b2f31496 731039e4977 8f54eee881, https://git.ke		
			A flaw was found in the ATA over Ethernet	rnel.org/stabl e/c/74ca3ef6 8d2f449bc84	

0-1

1-2

2-33-44-5Page 937 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(AoE) driver in the Linux	8c0a814cefc4 87bf755fa	
			kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on		
			`struct net_device`, and a use-after-free can be triggered by racing		
			between the free on the struct and the access through the `skbtxq`		
			global queue. This could lead to a denial of service condition or		
			potential code execution.		
			In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial		
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		

0-1

1-2

**2-3** 3-4 4-5 Page **938** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This patch removed the dev_put(ifp) in the success path in aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx(). CVE ID : CVE-2024- 26898		
Use of Uninitialize d Resource	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak syzbot identified a kernel information leak vulnerability in do_sys_name_to_handle () and issued the following report [1]. [1] "BUG: KMSAN: kernel- infoleak in instrument_copy_to_use r include/linux/instrume nted.h:114 [inline] BUG: KMSAN: kernel- infoleak in _copy_to_user+0xbc/0x 100 lib/usercopy.c:40 instrument_copy_to_use r	https://git.ke rnel.org/stabl e/c/3948abaa 4e2be938ccdf c289385a273 42fb13d43, https://git.ke rnel.org/stabl e/c/423b6bdf 19bbc5e1f7e7 46104509991 7378f7e71, https://git.ke rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228 a68d8a7c1	0-LIN-LINU- 030524/921

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/instrume nted.h:114 [inline]		
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40		
			copy_to_user include/linux/uaccess.h :191 [inline]		
			do_sys_name_to_handle fs/fhandle.c:73 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517		
			do_kmalloc_node mm/slab_common.c:10 06 [inline]		

0-1

1-2

**2-3** 3-4 4-5 Page **940** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kmalloc+0x121/0x3c 0 mm/slab_common.c:10 20		
			kmalloc include/linux/slab.h:60 4 [inline]		
			do_sys_name_to_handle fs/fhandle.c:39 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94 		
			Bytes 18-19 of 20 are uninitialized		
			Memory access of size 20 starts at ffff888128a46380		
			Data copied to user address 0000000020000240"		
			Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to		
			solve the problem.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 26901		
			In the Linux kernel, the following vulnerability has been resolved:		
			Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security		
			During our fuzz testing of the connection and disconnection process at the	https://git.ke rnel.org/stabl	
			RFCOMM layer, we discovered this bug. By comparing the packets from a normal connection and disconnection process	8fa0f42ddff3e 5255cf5e742c 9b77bb26,	
NULL Pointer Dereferenc	17-Apr-2024	5.5		0-LIN-LINU- 030524/922	
е			triggered a KASAN report. We analyzed the cause of this bug as follows:	429a202cde9 a73d3ae29b, https://git.ke rnel.org/stabl e/c/3ead59ba	
		1. In the packets captured during a normal connection, the host sends a	fad05f2967ae 2438c0528d5 3244cfde5		
			`Read Encryption Key Size` type of `HCI_CMD` packet		
			(Command Opcode: 0x1408) to the controller to inquire the length of		
			encryption key.After receiving this packet,		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the controller immediately		
			-		
			replies with a Command		
			Completepacket (Event		
			Code: 0x0e) to return		
			the		
			Encryption Key Size.		
			2. In our fuzz test case,		
			the timing of the		
			controller's response to		
			this		
			packet was delayed to		
			an unexpected point:		
			after the RFCOMM and L2CAP		
			layers had disconnected		
			but before the HCI layer		
			had disconnected.		
			3. After receiving the		
			Encryption Key Size		
			Response at the time		
			described		
			in point 2, the host still		
			called the		
			rfcomm_check_security function.		
			However, by this time		
			`struct l2cap_conn		
			*conn = l2cap_pi(sk)-		
			>chan->conn;`		
			had already been		
			released, and when the		
			function executed		
			`return		
			hci_conn_security(conn		
			->hcon, d->sec_level, auth_type, d->out);`,		
			aum_type, u->outj, ,		

0-1

1-2

2-33-44-5Page 943 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically when accessing `conn->hcon`, a null-ptr-deref error occurred.		
			To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling		
			rfcomm_recv_frame in rfcomm_process_rx.		
			CVE ID : CVE-2024- 26903		
Affected Ver	sion(s): From (i	ncluding)	5.5 Up to (excluding) 6.1.8	3	
Improper Locking	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix data race at btrfs_use_block_rsv() when accessing block reserve At btrfs_use_block_rsv() we read the size of a block reserve without locking its spinlock, which makes KCSAN complain because the size of a block reserve is always updated while holding its spinlock. The report from KCSAN is the following: [653.313148] BUG: KCSAN: data-race in btrfs_update_delayed_r	https://git.ke rnel.org/stabl e/c/2daa2a8e 895e6dc2395 f8628c011bcf 1e019040d, https://git.ke rnel.org/stabl e/c/7e9422d 35d574b6462 69ca46010a8 35ca074b310, https://git.ke rnel.org/stabl e/c/ab1be3f1 aa7799f9915 5488c28eacae f65eb68fb	0-LIN-LINU- 030524/923

0-1

1-2

**2-3** 3-4 4-5 Page **944** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			efs_rsv [btrfs] / btrfs_use_block_rsv [btrfs]		
			[653.314755] read to 0x000000017f5871b8 of 8 bytes by task 7519 on cpu 0: [653.314779]		
			btrfs_use_block_rsv+0x e4/0x2f8 [btrfs]		
			[653.315606] btrfs_alloc_tree_block+0 xdc/0x998 [btrfs]		
			[653.316421] btrfs_force_cow_block+ 0x220/0xe38 [btrfs]		
			[653.317242] btrfs_cow_block+0x1ac /0x568 [btrfs]		
			[653.318060] btrfs_search_slot+0xda 2/0x19b8 [btrfs]		
			[653.318879] btrfs_del_csums+0x1dc /0x798 [btrfs]		
			[653.319702] btrfs_free_extent.isra. 0+0xc24/0x2028 [btrfs]		
			[653.320538] btrfs_run_delayed_ref s+0xd3c/0x2390 [btrfs]		
			[653.321340] btrfs_run_delayed_refs+ 0xae/0x290 [btrfs]		
			[653.322140] flush_space+0x5e4/0x7 18 [btrfs]		

0-1

1-2

2-33-44-5Page 945 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.322958] btrfs_preempt_reclaim_ metadata_space+0x102 /0x2f8 [btrfs]		
			[653.323781] process_one_work+0x3 b6/0x838		
			[653.323800] worker_thread+0x75e/ 0xb10		
			[653.323817] kthread+0x21a/0x230		
			[653.323836] ret_from_fork+0x6c/0 xb8		
			[653.323855] ret_from_fork+0xa/0x3 0		
			[653.323887] write to 0x000000017f5871b8 of 8 bytes by task 576 on cpu 3:		
			[653.323906] btrfs_update_delayed_r efs_rsv+0x1a4/0x250 [btrfs]		
			[653.324699] btrfs_add_delayed_data _ref+0x468/0x6d8 [btrfs]		
			[653.325494] btrfs_free_extent+0x76 /0x120 [btrfs]		
			[653.326280] btrfs_mod_ref+0x6a8/ 0x6b8 [btrfs]		
			[653.327064] btrfs_dec_ref+0x50/0x7 0 [btrfs]		

0-1

1-2

2-3 3-4 4-5 Page **946** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.327849] walk_up_proc+0x236/0 xa50 [btrfs]		
			[653.328633] walk_up_tree+0x21c/0x 448 [btrfs]		
			[653.329418] btrfs_drop_snapshot+0x 802/0x1328 [btrfs]		
			[653.330205] btrfs_clean_one_deleted _snapshot+0x184/0x23 8 [btrfs]		
			[653.330995] cleaner_kthread+0x2b0 /0x2f0 [btrfs]		
			[653.331781] kthread+0x21a/0x230		
			[653.331800] ret_from_fork+0x6c/0 xb8		
			[653.331818] ret_from_fork+0xa/0x3 0		
			So add a helper to get the size of a block reserve while holding the lock.		
			Reading the field while holding the lock instead of using the data_race()		
			annotation is used in order to prevent load tearing.		
			CVE ID : CVE-2024- 26904		
Affected Ver	sion(s): From (i	ncluding)	5.9 Up to (excluding) 5.10	.146	

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness N/A		<b>CVSSv3</b>	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: Set lineevent_state::irq after IRQ register successfully When running gpio test on nxp-ls1028 platform with below command gpiomonnum- events=3rising-edge gpiochip1 25 There will be a warning trace as below: Call trace: free_irq+0x204/0x360 lineevent_free+0x64/0x 70 gpio_ioctl+0x598/0x6a	Patch           https://git.ke           rnel.org/stabl           e/c/657803b           918e097e47d           99d1489da83           a603c36bcdd,           https://git.ke           rnel.org/stabl           e/c/69bef19d           6b9700e9628           5f4b4e28691           cda3dcd0d1,           https://git.ke           rnel.org/stabl           e/c/97da736c           d11ae73bdf2f           5e21e24446b           8349e0168	O-LIN-LINU- 030524/924
			70		
			function failed, and then lineevent_free() is invoked to release		

CVSS Scoring Scale

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the resource. Since the lineevent_state::irq was already set, so		
			the subsequent invocation of free_irq() would trigger the above		
			warning call trace. To fix this issue, set the lineevent_state::irq		
			after the IRQ register successfully.		
			CVE ID : CVE-2022- 48660		
Affected Vers	sion(s): From (i	ncluding)	6.2 Up to (excluding) 6.6.1	.8	
			In the Linux kernel, the following vulnerability has been resolved:		
Concurrent			pmdomain: mediatek: fix race conditions with genpd	https://git.ke rnel.org/stabl e/c/339ddc9 83bc1622341	
Execution using Shared			If the power domains are registered first with genpd and *after that*	d95f244c361c da3da3a4ff, https://git.ke	
Resource with Improper	17-Apr-2024	4.7	the driver attempts to power them on in the	rnel.org/stabl e/c/3cd1d92e e1dbf3e8f988	O-LIN-LINU- 030524/925
Synchroniz			probe sequence, then it is	767eb75f262 07397792b,	
ation ('Race Condition')			possible that a race condition occurs if genpd tries to power them on	https://git.ke rnel.org/stabl e/c/475426a d1ae0bfdfd8f	
			in the same time.	160ed975090 3799392438	
			The same is valid for powering them off		
			before unregistering them		
			from genpd.		

0-1

1-2

2-3 3-4 4-5 Page **949** of **1051**  5-6

6-7

7-8 8-9

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		Attempt to fix race conditions by first removing the domains from genpd		
		and *after that* powering down domains.		
		Also first power up the domains and *after that* register them		
		to genpd.		
		CVE ID : CVE-2023- 52645		
		In the Linux kernel, the following vulnerability has been resolved:		
		netfilter: ipset: fix performance regression in swap operation	https://git.ke rnel.org/stabl e/c/653bc5e6 d9995d7d5f4	
		The patch "netfilter: ipset: fix race condition between swap/destroy	75a626161c, https://git.ke rnel.org/stabl	
17-Apr-2024	4.7	and kernel side add/del/test", commit 28628fa9 fixes a race condition	e/c/970709a 67696b100a5 7b33af1a3d7 5fc34b747eb,	0-LIN-LINU- 030524/926
		But the synchronize_rcu() added to the swap function unnecessarily slows	https://git.ke rnel.org/stabl e/c/97f7cf1cd 80eeed3b7c8 08b7c124632 95c751001	
		it down: it can safely be moved to destroy and use call_rcu() instead.		
			Image: 1 state of the state	17-Apr-20244.7Attempt to fix race conditions by first removing the domains from genpd and *after that* powering down domains.https://git.ke reliance is suppleted is suppleted and earlier is suppleted is suppleted 

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Eric Dumazet pointed out that simply calling the destroy functions as		
			rcu callback does not work: sets with timeout use garbage collectors		
			which need cancelling at destroy which can wait. Therefore the destroy		
			functions are split into two: cancelling garbage collectors safely at		
			executing the command received by netlink and moving the remaining		
			part only into the rcu callback.		
			CVE ID : CVE-2024- 26910		
Affected Ver	sion(s): From (i	ncluding)	6.2 Up to (excluding) 6.6.2	23	
		17-Apr-2024 <b>7.8</b>	In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/5c03387	
			net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv()	021cfa3336b 97e0dcba380 29917a8af2a, https://git.ke rnel.org/stabl e/c/60044ab	O-LIN-LINU-
N/A 17-Apr-20	17-Apr-2024		Apply the same fix than ones found in :	84836359534 bd7153b92e9 c1584140e4a,	030524/927
			8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in ip6_tnl_rcv()")	https://git.ke rnel.org/stabl e/c/77fd5294 ea09b21f677 2ac954a121b	
			1ca1ba465e55 ("geneve: make sure to	87323cec80	

0-1

1-2

2-33-44-5Page 951 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pull inner header in geneve_rx()")		
			We have to save skb- >network_header in a temporary variable		
			in order to be able to recompute the network_header pointer		
			after a pskb_inet_may_pull() call.		
			pskb_inet_may_pull() makes sure the needed headers are in skb- >head.		
			syzbot reported:		
			BUG: KMSAN: uninit-		
			value in INET_ECN_decapsulat		
			е		
			include/net/inet_ecn.h: 253 [inline]		
			BUG: KMSAN: uninit-		
			value in INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			BUG: KMSAN: uninit-		
			value in IP_ECN_decapsulate		
			include/net/inet_ecn.h: 302 [inline]		
			BUG: KMSAN: uninit-		
			value in		
			ip_tunnel_rcv+0xed9/0 x2ed0		

0-1

1-2

2-33-44-5Page 952 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/ipv4/ip_tunnel.c:40 9		
			INET_ECN_decapsulat e		
			include/net/inet_ecn.h: 253 [inline]		
			INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			ipgre_rcv+0x9bc/0xb c0 net/ipv4/ip_gre.c:389		
			ipgre_rcv net/ipv4/ip_gre.c:411 [inline]		
			gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447		
			gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c: 163		
			ip_protocol_deliver_rcu +0x264/0x1300 net/ipv4/ip_input.c:205		
			ip_local_deliver_finish+ 0x2b8/0x440 net/ipv4/ip_input.c:233		

0-1

1-2

2-33-44-5Page 953 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_local_deliver+0x21f/ 0x490 net/ipv4/ip_input.c:254		
			dst_input include/net/dst.h:461 [inline]		
			ip_rcv_finish net/ipv4/ip_input.c:449 [inline]		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569		
			netif_receive_skb_one _core net/core/dev.c:5534 [inline]		
			netif_receive_skb+0x1 a6/0x5a0 net/core/dev.c:5648		
			netif_receive_skb_intern al net/core/dev.c:5734 [inline]		
			netif_receive_skb+0x58 /0x660 net/core/dev.c:5793		
			tun_rx_batched+0x3ee/ 0x980 drivers/net/tun.c:1556		

0-1

1-2

3-4 4-5 2-3

8-9 7-8

9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tun_get_user+0x53b9/0 x66e0 drivers/net/tun.c:2009		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055 call_write_iter include/linux/fs.h:2087		
			[inline] new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			Uninit was created at:		
			alloc_pages+0x9a6/0x e00 mm/page_alloc.c:4590		
			alloc_pages_mpol+0x62 b/0x9d0 mm/mempolicy.c:2133		
			alloc_pages+0x1be/0x1 e0 mm/mempolicy.c:2204		
			skb_page_frag_refill+0x 2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline]		
			tun_get_user+0xe0a/0x 66e0 drivers/net/tun.c:1826		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		

0-1

1-2

**2-3** 3-4 4-5 Page **956** of **1051**  5-6

6-7

7-8 8-9 <mark>9-1</mark>0

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/comm		
			on.c:52 [inline] do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b <b>CVE ID : CVE-2024-</b>		
			26882		
Improper Restriction of			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/0971126 c8164abe200 4b8536b4969	
Operations within the Bounds of a Memory	17-Apr-2024	7.8	bpf: Fix stackmap overflow check on 32- bit arches	40853604969 0a0d6005b0a, https://git.ke rnel.org/stabl e/c/1564100	0-LIN-LINU- 030524/928
Buffer			The stackmap code relies on	7df0f0d35fa2 8742b25c2a7 db9dcd6895,	

0-1

1-2

2-33-44-5Page 957 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the	https://git.ke rnel.org/stabl e/c/21e5fa46 88e1a4d3db6 b72216231b2	
			resulting value is 0. However, on 32-bit arches, the roundup code itself	4232f75c1d	
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code.		
			The commit in the fixes tag actually attempted to fix this, but the fix		
			did not account for the UB, so the fix only works on CPUs where an		
			overflow does result in a neat truncation to zero, which is not		
			guaranteed. Checking the value before rounding does not have this		
			problem.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 26883		
			In the Linux kernel, the following vulnerability has been resolved:		
			bpf: Fix hashtab overflow check on 32- bit arches		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	bit arches The hashtab code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit arches, the roundup code itself can overflow by doing a 32-bit left-shift of an unsigned long value, which is undefined behaviour, so it is not guaranteed to truncate neatly. This was triggered by syzbot on the DEVMAP_HASH type, which contains the same check, copied from the hashtab code. So apply the same	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d 92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6 5f07b1132c1 979d73f014a e6e04de55d, https://git.ke rnel.org/stabl e/c/64f00b4d f0597590b19 9b62a37a165 473bf658a6	0-LIN-LINU- 030524/929
			fix to hashtab, by moving the overflow check to before the roundup.		

0-1

1-2

2-33-44-5Page 959 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 26884		
			In the Linux kernel, the following vulnerability has been resolved:		
			bpf: Fix DEVMAP_HASH overflow check on 32- bit arches		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	The devmap code allocates a number hash buckets equal to the next power of two of the max_entries value provided when creating the map. When rounding up to the next power of two, the 32-bit variable storing the number of buckets can overflow, and the code checks for overflow by checking if the truncated 32-bit value is equal to 0. However, on 32-bit	https://git.ke rnel.org/stabl e/c/22079b3 a423382335f 47d9ed32114 e6c9fe88d7c, https://git.ke rnel.org/stabl e/c/225da02 acdc97af01b6 bc6ce1a3e53 62bf01d3fb, https://git.ke rnel.org/stabl e/c/250051ac c21f9d4c5c59 5e4fcb55986e a08c4691	O-LIN-LINU- 030524/930
		arches the rounding up itself can overflow mid- way through, because it ends up doing a left-			
			shift of 32 bits on an unsigned long value. If the		
			size of an unsigned long is four bytes, this is undefined behaviour, so		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there is no guarantee that we'll end up with a nice and tidy 0-value at		
			the end.		
			Syzbot managed to turn this into a crash on arm32 by creating a		
			DEVMAP_HASH with max_entries > 0x80000000 and then trying to update it.		
			Fix this by moving the overflow check to before the rounding up		
			operation.		
			CVE ID : CVE-2024- 26885		
	17-Apr-2024 7.8		In the Linux kernel, the following vulnerability has been resolved:	https://git.ke	
			aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts	rnel.org/stabl e/c/079cba4f 4e307c69878 226fdf5228c2 0aa1c969c,	
Use After Free		7.8	This patch is against CVE-2023-6270. The description of cve is:	https://git.ke rnel.org/stabl e/c/1a54aa50 6b3b2f31496 731039e4977	O-LIN-LINU- 030524/931
			A flaw was found in the ATA over Ethernet (AoE) driver in the Linux	8f54eee881, https://git.ke rnel.org/stabl e/c/74ca3ef6 8d2f449bc84	
			kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on	8c0a814cefc4 87bf755fa	

0-1

1-2

2-33-44-5Page 961 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`struct net_device`, and a use-after-free can be triggered by racing		
			between the free on the struct and the access through the `skbtxq`		
			global queue. This could lead to a denial of service condition or		
			potential code execution.		
			In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial		
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		
			This patch removed the dev_put(ifp) in the success path in		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx().		
			CVE ID : CVE-2024- 26898		
			In the Linux kernel, the following vulnerability has been resolved:		
			RDMA/mlx5: Fix fortify source warning while accessing Eth segment		
			[ cut here ]	https://git.ke rnel.org/stabl	
N/A	17-Apr-2024	7.8	memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131 (size 2)	e/c/185fa070 00e0a81d54cf 8c05414cebff 14469a5c, https://git.ke rnel.org/stabl e/c/4d5e86a 56615cc387d 21c629f9af8f b0e958d350,	O-LIN-LINU- 030524/932
			WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131 mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]	https://git.ke rnel.org/stabl e/c/60ba938 a8bc8c90e72 4c75f98e932f 9fb7ae1b9d	
			Modules linked in: 8021q garp mrp stp llc rdma_ucm(OE) rdma_cm(OE) iw_cm(OE) ib_ipoib(OE) ib_cm(OE) ib_umad(OE) mlx5_ib(OE)		

0-1

1-2

2-33-44-5Page 963 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ib_uverbs(OE)		
			ib_core(OE)		
			mlx5_core(OE)		
			pci_hyperv_intf		
			mlxdevm(OE)		
			mlx_compat(OE) tls		
			mlxfw(OE) psample		
			nft_fib_inet nft_fib_ipv4		
			nft_fib_ipv6 nft_fib		
			nft_reject_inet		
			nf_reject_ipv4		
			nf_reject_ipv6 nft_reject		
			nft_ct nft_chain_nat		
			nf_nat nf_conntrack		
			nf_defrag_ipv6		
			nf_defrag_ipv4 ip_set		
			nf_tables libcrc32c		
			nfnetlink		
			mst_pciconf(OE)		
			knem(OE) vfio_pci		
			vfio_pci_core		
			vfio_iommu_type1 vfio		
			iommufd irqbypass		
			cuse nfsv3 nfs fscache		
			netfs xfrm_user		
			xfrm_algo ipmi_devintf		
			ipmi_msghandler		
			binfmt_misc		
			crct10dif_pclmul		
			crc32_pclmul		
			polyval_clmulni		
			polyval_generic		
			ghash_clmulni_intel		
			sha512_ssse3 snd_pcsp		
			aesni_intel crypto_simd		
			cryptd snd_pcm		
			snd_timer joydev snd		
			soundcore input_leds		
			serio_raw evbug nfsd		
			auth_rpcgss nfs_acl		
			lockd grace		
			sch_fq_codel sunrpc		
			drm efi_pstore ip_tables		
			x_tables autofs4		

0-1

1-2

2-3 3-4 4-5 Page 964 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			psmouse virtio_net net_failover failover floppy		
			[last unloaded: mlx_compat(OE)]		
			CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2.0-32-generic #32~22.04.1-Ubuntu		
			Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011		
			RIP: 0010:mlx5_ib_post_sen d+0x191b/0x1a60 [mlx5_ib]		
			Code: 0c 01 00 a8 01 75 25 48 8b 75 a0 b9 02 00 00 00 48 c7 c2 10 5b fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01 e8 95 4d 93 da <0f> 0b 44 8b 4d b0 4c 8b 45 c8 48 8b 4d c0 e9 49 fb ff ff 41 0f b7		
			RSP: 0018:ffffb5b48478b570 EFLAGS: 00010046		
			RAX: 000000000000000000 RBX: 00000000000000001 RCX: 000000000000000000000000000000000000		
			RDX: 000000000000000000 RSI: 000000000000000000000 RDI: 000000000000000000000000000000000000		

0-1

1-2

2-33-44-5Page 965 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000		
			R10: 0000000000000000000 R11: 0000000000		
			R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80		
			FS: 00007fc03b444c80(00 00) GS:ffff963a3dc00000(0 000) knlGS:0000000000000 000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			CR2: 0000556f46bdf000 CR3: 000000006ac6003 CR4: 0000000003706f0		
			DR0: 0000000000000000 DR1: 00000000000000000 DR2: 000000000000000000000000000000000000		
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		

0-1

1-2

2-3 3-4 4-5 Page 966 of 1051 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<task></task>		
			?		
			show_regs+0x72/0x90		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?_warn+0x8d/0x160		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?		
			report_bug+0x1bb/0x1 d0		
			?		
			handle_bug+0x46/0x90		
			?		
			exc_invalid_op+0x19/0 x80		
			?		
			asm_exc_invalid_op+0x 1b/0x20		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			mlx5_ib_post_send_nod		
			rain+0xb/0x20 [mlx5_ib]		
			ipoib_send+0x2ec/0x77 0 [ib_ipoib]		
			ipoib_start_xmit+0x5a0 /0x770 [ib_ipoib]		
			dev_hard_start_xmit+0x 8e/0x1e0		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? validate_xmit_skb_list+ 0x4d/0x80		
			sch_direct_xmit+0x116 /0x3a0		
			dev_xmit_skb+0x1fd/ 0x580		
			dev_queue_xmit+0x28 4/0x6b0 ?		
			_raw_spin_unlock_irq+0 xe/0x50		
			? flush_work.isra.0+0x2 0d/0x370 ?		
			? push_pseudo_header+0 x17/0x40 [ib_ipoib]		
			neigh_connected_outpu t+0xcd/0x110		
			ip_finish_output2+0x17 9/0x480		
			? smp_call_single_queue +0x61/0xa0		
			ip_finish_output+0xc3 /0x190		
			ip_finish_output+0x2e/ 0xf0		
			ip_output+0x78/0x110		

0-1

1-2

5-6

6-7

 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_ip_finish_output+ 0x10/0x10		
			ip_local_out+0x64/0x7 0		
			ip_queue_xmit+0x18a /0x460		
			ip_queue_xmit+0x15/0 x30		
			tcp_transmit_skb+0x9 14/0x9c0		
			tcp_write_xmit+0x334/ 0x8d0		
			tcp_push_one+0x3c/0x 60		
			tcp_sendmsg_locked+0x 2e1/0xac0		
			tcp_sendmsg+0x2d/0x5		
			inet_sendmsg+0x43/0x 90 sock_sendmsg+0x68/0x		
			sock_sendinsg+0x68/0x 80 sock_write_iter+0x93/0		
			x100 vfs_write+0x326/0x3c0		
			ksys_write+0xbd/0xf0		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_syscall_64+0x69/0x 90		
			x64_sys_write+0x19/ 0x30 do_syscall_ truncated <b>CVE ID : CVE-2024-</b> 26907		
NULL Pointer Dereferenc e	17-Apr-2024	5.5	26907 In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when 1588 is received on HIP08 devices The HIP08 devices does not register the ptp devices, so the hdev->ptp is NULL, but the hardware can receive 1588 messages, and set the HNS3_RXD_TS_VLD_B bit, so, if match this case, the access of hdev->ptp- >flags will cause a kernel crash: [ 5888.946472] Unable to handle kernel NULL pointer dereference at virtual address	https://git.ke rnel.org/stabl e/c/0fbcf236 6ba9888cf02e da23e35fde7f 7fcc07c3, https://git.ke rnel.org/stabl e/c/11b9983 60d96f6c76f0 4a95f54b49f2 4d3c858e4, https://git.ke rnel.org/stabl e/c/23ec1cec 24293f9799c 725941677d4 e167997265	0-LIN-LINU- 030524/933

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 00000000000018		
			 [ 5889.266118] pc : hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge] [ 5889.272612] lr : hclge_ptp_get_rx_hwts+ 0x34/0x170 [hclge] [ 5889.279101] sp : ffff800012c3bc50		
			[ 5889.283516] x29: ffff800012c3bc50 x28: ffff2040002be040		
			[ 5889.289927] x27: ffff800009116484 x26: 0000000080007500		
			[ 5889.296333] x25: 0000000000000000 x24: ffff204001c6f000 [ 5889.302738] x23:		
			ffff204144f53c00 x22: 00000000000000000 [ 5889.309134] x21:		
			[ 5009.30913 1] x21: 00000000000000000 x20: ffff204004220080 [ 5889.315520] x19:		
			ffff204144f53c00 x18: 00000000000000000 [ 5889.321897] x17:		
			000000000000000000 x16: 000000000000000000000		
			[ 5889.328263] x15: 0000004000140ec8 x14: 00000000000000000		

0-1

1-2

2-33-44-5Page 971 of 1051

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.334617] x13: 00000000000000000 x12: 00000000010011df		
			[ 5889.340965] x11: bbfeff4d22000000 x10: 000000000000000000		
			[ 5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d		
			[ 5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480		
			[ 5889.359959] x5 : 0000000000000000 x4 : 00000000000000000		
			[ 5889.366271] x3 : 000000000000000 x2 : 00000000000000000		
			[ 5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		
			[ 5889.378857] Call trace:		
			[ 5889.382285] hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.388304] hns3_handle_bdinfo+0x 324/0x410 [hns3]		
			[ 5889.394055] hns3_handle_rx_bd+0x6 0/0x150 [hns3]		
			[ 5889.399624] hns3_clean_rx_ring+0x8 4/0x170 [hns3]		
			[ 5889.405270] hns3_nic_common_poll +0xa8/0x220 [hns3]		

0-1

1-2

2-33-44-5Page 972 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.411084] napi_poll+0xcc/0x264 [ 5889.415329] net_rx_action+0xd4/0x 21c		
			[ 5889.419911] do_softirq+0x130/0x 358		
			[ 5889.424484] irq_exit+0x134/0x154		
			[ 5889.428700] handle_domain_irq+0 x88/0xf0		
			[ 5889.433684] gic_handle_irq+0x78/0 x2c0		
			[ 5889.438319] el1_irq+0xb8/0x140		
			[ 5889.442354] arch_cpu_idle+0x18/0x 40		
			[ 5889.446816] default_idle_call+0x5c/ 0x1c0		
			[ 5889.451714] cpuidle_idle_call+0x174 /0x1b0		
			[ 5889.456692] do_idle+0xc8/0x160		
			[ 5889.460717] cpu_startup_entry+0x3 0/0xfc		
			[ 5889.465523] secondary_start_kernel +0x158/0x1ec		
			[ 5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80)		

0-1

1-2

2-33-44-5Page 973 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.477950] SMP: stopping secondary CPUs		
			[ 5890.514626] SMP: failed to stop secondary CPUs 0-69,71-95		
			[ 5890.522951] Starting crashdump kernel		
			CVE ID : CVE-2024- 26881		
			In the Linux kernel, the following vulnerability has been resolved:		
Use of Uninitialize 17-A			do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak	https://git.ke	
	17-Apr-2024	17-Apr-2024 5.5	vulnerability in do_sys_name_to_hand () and issued the following report [1].	kernel information leak vulnerability in do_sys_name_to_handle () and issued the	rnel.org/stabl e/c/3948abaa 4e2be938ccdf c289385a273 42fb13d43, https://git.ke rnel.org/stabl e/c/423b6bdf
d Resource	F -		[1] "BUG: KMSAN: kernel- infoleak in instrument_copy_to_use r include/linux/instrume nted.h:114 [inline] BUG: KMSAN: kernel- infoleak in _copy_to_user+0xbc/0x 100 lib/usercopy.c:40	19bbc5e1f7e7 46104509991 7378f7e71, https://git.ke rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228 a68d8a7c1	030524/934
			instrument_copy_to_use r		

0-1

1-2

2-33-44-5Page 974 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/instrume nted.h:114 [inline]		
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40		
			copy_to_user include/linux/uaccess.h :191 [inline]		
			do_sys_name_to_handle fs/fhandle.c:73 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517		
			do_kmalloc_node mm/slab_common.c:10 06 [inline]		

0-1

1-2

2-33-44-5Page 975 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_kmalloc+0x121/0x3c 0 mm/slab_common.c:10 20		
			kmalloc include/linux/slab.h:60 4 [inline]		
			do_sys_name_to_handle fs/fhandle.c:39 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94 		
			Bytes 18-19 of 20 are uninitialized		
			Memory access of size 20 starts at ffff888128a46380		
			Data copied to user address 0000000020000240"		
			Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to		
			solve the problem.		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2024- 26901			
			In the Linux kernel, the following vulnerability has been resolved:			
			Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security			
			During our fuzz testing of the connection and disconnection process at the	https://git.ke rnel.org/stabl		
	17-Apr-2024 5.5	RFCOMM layer, we discovered this bug. By comparing the packets from a	FCOMM layer, we iscovered this bug. By omparing the packetse/c/2535b84 8fa0f42ddff3e 5255cf5e742c ob77bb26			
NULL Pointer Dereferenc		4 5.5	5.5	normal connection and disconnection process with the testcase that	https://git.ke rnel.org/stabl e/c/369f419c 097e82407dd	O-LIN-LINU- 030524/935
e				triggered a KASAN report. We analyzed the cause of this bug as follows:	429a202cde9 a73d3ae29b, https://git.ke rnel.org/stabl e/c/3ead59ba	
		1. In the packets captured during a normal connection, the host sends a	fad05f2967ae 2438c0528d5 3244cfde5			
			`Read Encryption Key Size` type of `HCI_CMD` packet			
			(Command Opcode: 0x1408) to the controller to inquire the length of			
			encryption key.After receiving this packet,			

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the controller		
			immediately		
			replies with a Command		
			Completepacket (Event		
			Code: 0x0e) to return		
			the		
			Encryption Key Size.		
			2. In our fuzz test case,		
			the timing of the		
			controller's response to		
			this		
			packet was delayed to		
			an unexpected point:		
			after the RFCOMM and L2CAP		
			layers had disconnected		
			but before the HCI layer		
			had disconnected.		
			3. After receiving the		
			Encryption Key Size		
			Response at the time		
			described		
			in point 2, the host still		
			called the rfcomm_check_security		
			function.		
			However, by this time		
			`struct l2cap_conn		
			*conn = l2cap_pi(sk)-		
			>chan->conn;`		
			had already been		
			released, and when the		
			function executed		
			`return		
			hci_conn_security(conn ->hcon, d->sec_level,		
			auth_type, d->out);`,		
			- , , , , ,		

0-1

1-2

2-33-44-5Page 978 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically when accessing `conn->hcon`, a null-ptr-deref error occurred.		
			To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling		
			rfcomm_recv_frame in rfcomm_process_rx.		
			CVE ID : CVE-2024- 26903		
Improper Locking	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix data race at btrfs_use_block_rsv() when accessing block reserve At btrfs_use_block_rsv() we read the size of a block reserve without locking its spinlock, which makes KCSAN complain because the size of a block reserve is always updated while holding its spinlock. The report from KCSAN is the following: [653.313148] BUG: KCSAN: data-race in btrfs_update_delayed_r	https://git.ke rnel.org/stabl e/c/2daa2a8e 895e6dc2395 f8628c011bcf 1e019040d, https://git.ke rnel.org/stabl e/c/7e9422d 35d574b6462 69ca46010a8 35ca074b310, https://git.ke rnel.org/stabl e/c/ab1be3f1 aa7799f9915 5488c28eacae f65eb68fb	O-LIN-LINU- 030524/936

0-1

1-2

2-33-44-5Page 979 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			btrfs_use_block_rsv [btrfs]		
			[653.314755] read to 0x000000017f5871b8 of 8 bytes by task 7519 on cpu 0:		
			[653.314779] btrfs_use_block_rsv+0x e4/0x2f8 [btrfs]		
			[653.315606] btrfs_alloc_tree_block+0 xdc/0x998 [btrfs]		
			[653.316421] btrfs_force_cow_block+ 0x220/0xe38 [btrfs]		
			[653.317242] btrfs_cow_block+0x1ac /0x568 [btrfs]		
			[653.318060] btrfs_search_slot+0xda 2/0x19b8 [btrfs]		
			[653.318879] btrfs_del_csums+0x1dc /0x798 [btrfs]		
			[653.319702] btrfs_free_extent.isra. 0+0xc24/0x2028 [btrfs]		
			[653.320538] btrfs_run_delayed_ref s+0xd3c/0x2390 [btrfs]		
			[653.321340] btrfs_run_delayed_refs+ 0xae/0x290 [btrfs]		
			[653.322140] flush_space+0x5e4/0x7 18 [btrfs]		
			[653.322958] btrfs_preempt_reclaim_		

0-1

1-2

**2-3** 3-4 4-5 Page **980** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			metadata_space+0x102 /0x2f8 [btrfs]		
			[653.323781]		
			process_one_work+0x3 b6/0x838		
			[653.323800] worker_thread+0x75e/ 0xb10		
			[653.323817] kthread+0x21a/0x230		
			[653.323836] ret_from_fork+0x6c/0 xb8		
			[653.323855] ret_from_fork+0xa/0x3 0		
			[653.323887] write to 0x000000017f5871b8 of 8 bytes by task 576 on cpu 3:		
			[653.323906] btrfs_update_delayed_r efs_rsv+0x1a4/0x250 [btrfs]		
			[653.324699] btrfs_add_delayed_data _ref+0x468/0x6d8 [btrfs]		
			[653.325494] btrfs_free_extent+0x76 /0x120 [btrfs]		
			[653.326280] btrfs_mod_ref+0x6a8/ 0x6b8 [btrfs]		
			[653.327064] btrfs_dec_ref+0x50/0x7 0 [btrfs]		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			[653.327849] walk_up_proc+0x236/0 xa50 [btrfs]					
			[653.328633] walk_up_tree+0x21c/0x 448 [btrfs]					
			[653.329418] btrfs_drop_snapshot+0x 802/0x1328 [btrfs]					
			[653.330205] btrfs_clean_one_deleted _snapshot+0x184/0x23 8 [btrfs]					
			[653.330995] cleaner_kthread+0x2b0 /0x2f0 [btrfs]					
			[653.331781] kthread+0x21a/0x230					
			[653.331800] ret_from_fork+0x6c/0 xb8					
			[653.331818] ret_from_fork+0xa/0x3 0					
			So add a helper to get the size of a block reserve while holding the lock.					
			Reading the field while holding the lock instead of using the data_race()					
			annotation is used in order to prevent load tearing.					
			CVE ID : CVE-2024- 26904					
Affected Vers	Affected Version(s): From (including) 6.3 Up to (excluding) 6.6.23							

0-1

1-2

2-33-44-5Page 982 of 1051

5-6

6-7

 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness Use After Free	Publish Date	CVSSv3	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink_altmode: fix drm bridge use-after- free A recent DRM series purporting to simplify support for "transparent bridges" and handling of probe deferrals ironically exposed a use-after-free issue on pmic_glink_altmode probe deferral.	Patch https://git.ke rnel.org/stabl e/c/2bbd65c 6ca567ed8db bfc4fb945f57 ce64bef342, https://git.ke rnel.org/stabl e/c/b979f2d5 0a099f34024 18d7ff5f26c3 952fb08bb,	NCIIPC ID
			subsystem occasionally failing to initialise and NULL- pointer dereferences during boot of machines like the Lenovo ThinkPad	https://git.ke rnel.org/stabl e/c/ef45aa28 41e15b649e5 417fe3d4de3 95fe462781	
			X13s.		
			Specifically, the dp-hpd bridge is currently registered before all		
			resources have been acquired which means that it can also be		
			deregistered on probe deferrals.		

0-1

1-2

2-33-44-5Page 983 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In the meantime there is a race window where the new aux bridge driver		
			(or PHY driver previously) may have looked up the dp-hpd bridge and		
			stored a (non- reference-counted) pointer to the bridge which is about to		
			be deallocated.		
			When the display controller is later initialised, this triggers a		
			use-after-free when attaching the bridges:		
			dp -> aux -> dp- hpd (freed)		
			which may, for example, result in the freed bridge failing to attach:		
			[drm:drm_bridg e_attach [drm]] *ERROR* failed to attach bridge /soc@0/phy@88eb000 to encoder TMDS-31: - 16		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or a NULL-pointer dereference:		
			Unable to handle kernel NULL pointer dereference at virtual address 00000000000000000000000000000000000		
			Call trace:		
			drm_bridge_attach+0x7 0/0x1a8 [drm]		
			drm_aux_bridge_attach +0x24/0x38 [aux_bridge]		
			drm_bridge_attach+0x8 0/0x1a8 [drm]		
			dp_bridge_init+0xa8/0x 15c [msm]		
			msm_dp_modeset_init+ 0x28/0xc4 [msm]		
			The DRM bridge implementation is clearly fragile and implicitly built on		
			the assumption that bridges may never go away. In this case, the fix is		
			to move the bridge registration in the pmic_glink_altmode driver to		

0-1

1-2

2-33-44-5Page 985 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after all resources have been looked up.		
			Incidentally, with the new dp-hpd bridge implementation, which registers		
			child devices, this is also a requirement due to a long-standing issue		
			in driver core that can otherwise lead to a probe deferral loop (see		
			commit fbc35b45f9f6 ("Add documentation on meaning of - EPROBE_DEFER")).		
			[DB: slightly fixed commit message by adding the word 'commit']		
			CVE ID : CVE-2024- 26909		
Affected Ver	sion(s): From (i	ncluding)	6.7 Up to (excluding) 6.7.1	.1	
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/5c03387 021cfa3336b	
N/A	17-Apr-2024	7.8	net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv()	97e0dcba380 29917a8af2a, https://git.ke rnel.org/stabl e/c/60044ab 84836359534	O-LIN-LINU- 030524/938
			Apply the same fix than ones found in :	bd7153b92e9 c1584140e4a, https://git.ke rnel.org/stabl	
			8d975c15c0cd ("ip6_tunnel: make sure	e/c/77fd5294 ea09b21f677	
CV/SS Scoring S					9.0 0.10

0-1

1-2

**2-3** 3-4 4-5 Page **986** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to pull inner header in ip6_tnl_rcv()") 1ca1ba465e55 ("geneve: make sure to pull inner header in geneve_rx()")	2ac954a121b 87323cec80	
			We have to save skb- >network_header in a temporary variable		
			in order to be able to recompute the network_header pointer		
			after a pskb_inet_may_pull() call.		
			pskb_inet_may_pull() makes sure the needed headers are in skb- >head.		
			syzbot reported: BUG: KMSAN: uninit- value in INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			BUG: KMSAN: uninit- value in INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			BUG: KMSAN: uninit- value in IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		

0-1

1-2

2-33-44-5Page 987 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KMSAN: uninit- value in ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline] INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			ipgre_rcv+0x9bc/0xb c0 net/ipv4/ip_gre.c:389 ipgre_rcv net/ipv4/ip_gre.c:411 [inline]		
			gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447 gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c: 163		
			ip_protocol_deliver_rcu +0x264/0x1300 net/ipv4/ip_input.c:205		
			ip_local_deliver_finish+		

0-1

1-2

**2-3** 3-4 4-5 Page **988** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x2b8/0x440 net/ipv4/ip_input.c:233 NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_local_deliver+0x21f/ 0x490 net/ipv4/ip_input.c:254 dst_input		
			include/net/dst.h:461 [inline]		
			ip_rcv_finish net/ipv4/ip_input.c:449 [inline]		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569		
			netif_receive_skb_one _core net/core/dev.c:5534 [inline]		
			netif_receive_skb+0x1 a6/0x5a0 net/core/dev.c:5648		
			netif_receive_skb_intern al net/core/dev.c:5734 [inline]		
			netif_receive_skb+0x58 /0x660 net/core/dev.c:5793		
			tun_rx_batched+0x3ee/		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x980		
			drivers/net/tun.c:1556		
			tun get user Orf2h0 (0		
			tun_get_user+0x53b9/0 x66e0		
			drivers/net/tun.c:2009		
			tun_chr_write_iter+0x3		
			af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter		
			include/linux/fs.h:2087		
			[inline]		
			new_sync_write		
			fs/read_write.c:497 [inline]		
			luuuel		
			vfs_write+0xb6b/0x15		
			20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write		
			fs/read_write.c:655		
			[inline]		
			se_sys_write		
			fs/read_write.c:652		
			[inline]		
			x64_sys_write+0x93/		
			0xd0		
			fs/read_write.c:652		
			do_syscall_x64		
			arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1		
			e0		
			arch/x86/entry/comm on.c:83		

0-1

1-2

**2-3** 3-4 4-5 Page **990** of **1051**  6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			Uninit was created at:		
			alloc_pages+0x9a6/0x e00 mm/page_alloc.c:4590		
			alloc_pages_mpol+0x62 b/0x9d0 mm/mempolicy.c:2133		
			alloc_pages+0x1be/0x1 e0 mm/mempolicy.c:2204		
			skb_page_frag_refill+0x 2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline]		
			tun_get_user+0xe0a/0x 66e0 drivers/net/tun.c:1826		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		

0-1

1-2

3-4 4-5 2-3 Page **991** of **1051** 

7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/comm		
			on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			CVE ID : CVE-2024- 26882		
Improper Restriction of			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/0971126 c8164abe200	
Operations within the Bounds of a Memory	17-Apr-2024	7.8	bpf: Fix stackmap overflow check on 32- bit arches	4b8536b4969 0a0d6005b0a, https://git.ke rnel.org/stabl e/c/1564100	O-LIN-LINU- 030524/939
Buffer			The stackmap code relies on	7df0f0d35fa2 8742b25c2a7 db9dcd6895,	

0-1

1-2

2-33-44-5Page 992 of 1051

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the	https://git.ke rnel.org/stabl e/c/21e5fa46 88e1a4d3db6 b72216231b2	
			resulting value is 0. However, on 32-bit arches, the roundup code itself	4232f75c1d	
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code.		
			The commit in the fixes tag actually attempted to fix this, but the fix		
			did not account for the UB, so the fix only works on CPUs where an		
			overflow does result in a neat truncation to zero, which is not		
			guaranteed. Checking the value before rounding does not have this		
			problem.		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 26883		
			In the Linux kernel, the following vulnerability has been resolved:		
			bpf: Fix hashtab overflow check on 32- bit arches		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	bit arches The hashtab code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit arches, the roundup code itself can overflow by doing a 32-bit left-shift of an unsigned long value, which is undefined behaviour, so it is not guaranteed to truncate neatly. This was triggered by syzbot on the DEVMAP_HASH type, which contains the same check, copied from the hashtab code. So apply the same fix to hashtab, by moving the overflow check to before the roundup.	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d 92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6 5f07b1132c1 979d73f014a e6e04de55d, https://git.ke rnel.org/stabl e/c/64f00b4d f0597590b19 9b62a37a165 473bf658a6	O-LIN-LINU- 030524/940

0-1

1-2

**2-3** 3-4 4-5 Page **994** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 26884		
			In the Linux kernel, the following vulnerability has been resolved:		
			bpf: Fix DEVMAP_HASH overflow check on 32- bit arches		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	The devmap code allocates a number hash buckets equal to the next power of two of the max_entries value provided when creating the map. When rounding up to the next power of two, the 32-bit variable storing the number of buckets can overflow, and the code checks for overflow by checking if the truncated 32-bit value is equal to 0. However, on 32-bit arches the rounding up itself can overflow mid- way through, because it	https://git.ke rnel.org/stabl e/c/22079b3 a423382335f 47d9ed32114 e6c9fe88d7c, https://git.ke rnel.org/stabl e/c/225da02 acdc97af01b6 bc6ce1a3e53 62bf01d3fb, https://git.ke rnel.org/stabl e/c/250051ac c21f9d4c5c59 5e4fcb55986e a08c4691	O-LIN-LINU- 030524/941
			ends up doing a left- shift of 32 bits on an unsigned long value. If the		
			size of an unsigned long is four bytes, this is undefined behaviour, so		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there is no guarantee that we'll end up with a nice and tidy 0-value at		
			the end.		
			Syzbot managed to turn this into a crash on arm32 by creating a		
			DEVMAP_HASH with max_entries > 0x80000000 and then trying to update it.		
			Fix this by moving the overflow check to before the rounding up		
			operation.		
			CVE ID : CVE-2024- 26885		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke	
	17-Apr-2024 7.8		aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts	rnel.org/stabl e/c/079cba4f 4e307c69878 226fdf5228c2 0aa1c969c,	
Use After Free		7.8	This patch is against CVE-2023-6270. The description of cve is:	https://git.ke rnel.org/stabl e/c/1a54aa50 6b3b2f31496 731039e4977	O-LIN-LINU- 030524/942
			A flaw was found in the ATA over Ethernet (AoE) driver in the Linux	8f54eee881, https://git.ke rnel.org/stabl e/c/74ca3ef6 8d2f449bc84	
			kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on	8c0a814cefc4 87bf755fa	

0-1

1-2

2-33-44-5Page 996 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`struct net_device`, and a use-after-free can be triggered by racing		
			between the free on the struct and the access through the `skbtxq`		
			global queue. This could lead to a denial of service condition or		
			potential code execution.		
			In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial		
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		
			This patch removed the dev_put(ifp) in the success path in		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx().		
			CVE ID : CVE-2024- 26898		
			In the Linux kernel, the following vulnerability has been resolved:		
			RDMA/mlx5: Fix fortify source warning while accessing Eth segment		
			[ cut here ]  memcpy: detected	https://git.ke rnel.org/stabl	
			field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx- ofed-	e/c/185fa070 00e0a81d54cf 8c05414cebff 14469a5c, https://git.ke rnel.org/stabl e/c/4d5e86a	O-LIN-LINU-
N/A	17-Apr-2024	7.8	kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131 (size 2)	56615cc387d 21c629f9af8f b0e958d350,	030524/943
		WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx- ofed- kernel/5.8/build/drive rs/infiniband/hw/mlx5 /wr.c:131 mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]	https://git.ke rnel.org/stabl e/c/60ba938 a8bc8c90e72 4c75f98e932f 9fb7ae1b9d		
			Modules linked in: 8021q garp mrp stp llc rdma_ucm(OE) rdma_cm(OE) iw_cm(OE) ib_ipoib(OE) ib_cm(OE) ib_umad(OE) mlx5_ib(OE)		

0-1

1-2

**2-3** 3-4 4-5 Page **998** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ib_uverbs(OE)		
			ib_core(OE)		
			mlx5_core(OE)		
			pci_hyperv_intf		
			mlxdevm(OE)		
			mlx_compat(OE) tls		
			mlxfw(OE) psample		
			nft_fib_inet nft_fib_ipv4		
			nft_fib_ipv6 nft_fib		
			nft_reject_inet		
			nf_reject_ipv4		
			nf_reject_ipv6 nft_reject		
			nft_ct nft_chain_nat		
			nf_nat nf_conntrack		
			nf_defrag_ipv6		
			nf_defrag_ipv4 ip_set		
			nf_tables libcrc32c		
			nfnetlink		
			mst_pciconf(OE)		
			knem(OE) vfio_pci		
			vfio_pci_core		
			vfio_iommu_type1 vfio		
			iommufd irqbypass		
			cuse nfsv3 nfs fscache		
			netfs xfrm_user		
			xfrm_algo ipmi_devintf		
			ipmi_msghandler		
			binfmt_misc		
			crct10dif_pclmul		
			crc32_pclmul		
			polyval_clmulni		
			polyval_generic		
			ghash_clmulni_intel		
			sha512_ssse3 snd_pcsp		
			aesni_intel crypto_simd		
			cryptd snd_pcm		
			snd_timer joydev snd		
			soundcore input_leds		
			serio_raw evbug nfsd		
			auth_rpcgss nfs_acl		
			lockd grace		
			sch_fq_codel sunrpc		
			drm efi_pstore ip_tables		
			x_tables autofs4		

0-1

1-2

**2-3** 3-4 4-5 Page **999** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			psmouse virtio_net net_failover failover floppy		
			[last unloaded: mlx_compat(OE)]		
			CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2.0-32-generic #32~22.04.1-Ubuntu		
			Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011		
			RIP: 0010:mlx5_ib_post_sen d+0x191b/0x1a60 [mlx5_ib]		
			Code: 0c 01 00 a8 01 75 25 48 8b 75 a0 b9 02 00 00 00 48 c7 c2 10 5b fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01 e8 95 4d 93 da <0f> 0b 44 8b 4d b0 4c 8b 45 c8 48 8b 4d c0 e9 49 fb ff ff 41 0f b7		
			RSP: 0018:ffffb5b48478b570 EFLAGS: 00010046		
			RAX: 000000000000000000 RBX: 00000000000000001 RCX: 000000000000000000000000000000000000		
			RDX: 000000000000000000 RSI: 000000000000000000000 RDI: 000000000000000000000000000000000000		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000		
			R10: 0000000000000000000 R11: 0000000000		
			R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80		
			FS: 00007fc03b444c80(00 00) GS:ffff963a3dc00000(0 000) knlGS:0000000000000 000		
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		
			CR2: 0000556f46bdf000 CR3: 000000006ac6003 CR4: 0000000003706f0		
			DR0: 0000000000000000 DR1: 00000000000000000 DR2: 000000000000000000000000000000000000		
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000000400		
			Call Trace:		

0-1

1-2

2-3 3-4 4-5 Page 1001 of 1051 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<task></task>		
			?		
			show_regs+0x72/0x90		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?_warn+0x8d/0x160		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			?		
			report_bug+0x1bb/0x1 d0		
			?		
			handle_bug+0x46/0x90		
			?		
			exc_invalid_op+0x19/0 x80		
			?		
			asm_exc_invalid_op+0x 1b/0x20		
			?		
			mlx5_ib_post_send+0x1 91b/0x1a60 [mlx5_ib]		
			mlx5_ib_post_send_nod		
			rain+0xb/0x20 [mlx5_ib]		
			ipoib_send+0x2ec/0x77 0 [ib_ipoib]		
			ipoib_start_xmit+0x5a0 /0x770 [ib_ipoib]		
			dev_hard_start_xmit+0x 8e/0x1e0		

0-1

1-2

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? validate_xmit_skb_list+ 0x4d/0x80		
			sch_direct_xmit+0x116 /0x3a0		
			dev_xmit_skb+0x1fd/ 0x580		
			dev_queue_xmit+0x28 4/0x6b0 ?		
			_raw_spin_unlock_irq+0 xe/0x50 ?		
			flush_work.isra.0+0x2 0d/0x370		
			? push_pseudo_header+0 x17/0x40 [ib_ipoib]		
			neigh_connected_outpu t+0xcd/0x110		
			ip_finish_output2+0x17 9/0x480 ?		
			? smp_call_single_queue +0x61/0xa0		
			ip_finish_output+0xc3 /0x190		
			ip_finish_output+0x2e/ 0xf0		
			ip_output+0x78/0x110		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? pfx_ip_finish_output+ 0x10/0x10		
			ip_local_out+0x64/0x7 0		
			ip_queue_xmit+0x18a /0x460		
			ip_queue_xmit+0x15/0 x30		
			tcp_transmit_skb+0x9 14/0x9c0		
			tcp_write_xmit+0x334/ 0x8d0		
			tcp_push_one+0x3c/0x 60		
			tcp_sendmsg_locked+0x 2e1/0xac0		
			tcp_sendmsg+0x2d/0x5 0		
			inet_sendmsg+0x43/0x 90		
			sock_sendmsg+0x68/0x 80		
			sock_write_iter+0x93/0 x100 vfs_write+0x326/0x3c0		
			ksys_write+0xbd/0xf0		
l			5		

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_syscall_64+0x69/0x 90		
			x64_sys_write+0x19/ 0x30 do_syscall_ truncated <b>CVE ID : CVE-2024-</b> 26907		
NULL Pointer Dereferenc e	17-Apr-2024	5.5	26907 In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when 1588 is received on HIP08 devices The HIP08 devices does not register the ptp devices, so the hdev->ptp is NULL, but the hardware can receive 1588 messages, and set the HNS3_RXD_TS_VLD_B bit, so, if match this case, the access of hdev->ptp- >flags will cause a kernel crash: [ 5888.946472] Unable to handle kernel NULL pointer dereference at virtual address	https://git.ke rnel.org/stabl e/c/0fbcf236 6ba9888cf02e da23e35fde7f 7fcc07c3, https://git.ke rnel.org/stabl e/c/11b9983 60d96f6c76f0 4a95f54b49f2 4d3c858e4, https://git.ke rnel.org/stabl e/c/23ec1cec 24293f9799c 725941677d4 e167997265	O-LIN-LINU- 030524/944

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 000000000000018		
			 [ 5889.266118] pc : hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.272612] lr : hclge_ptp_get_rx_hwts+ 0x34/0x170 [hclge] [ 5889.279101] sp :		
			ffff800012c3bc50 [ 5889.283516] x29: ffff800012c3bc50 x28:		
			ffff2040002be040 [ 5889.289927] x27: ffff800009116484 x26: 0000000080007500		
			[ 5889.296333] x25: 00000000000000000 x24: ffff204001c6f000		
			[ 5889.302738] x23: ffff204144f53c00 x22: 00000000000000000		
			[ 5889.309134] x21: 0000000000000000 x20: ffff204004220080		
			[ 5889.315520] x19: ffff204144f53c00 x18: 0000000000000000		
			[ 5889.321897] x17: 00000000000000000 x16: 000000000000000000000000000000000000		
			[ 5889.328263] x15: 0000004000140ec8 x14:		
			0000004000140ec8		

0-1

1-2

2-3 3-4 4-5 Page 1006 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.334617] x13: 00000000000000000 x12: 00000000010011df		
			[ 5889.340965] x11: bbfeff4d22000000 x10: 00000000000000000		
			[ 5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d		
			[ 5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480		
			[ 5889.359959] x5 : 0000000000000000 x4 : 000000000000000000		
			[ 5889.366271] x3 : 000000000000000 x2 : 00000000000000000		
			[ 5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		
			[ 5889.378857] Call trace:		
			[ 5889.382285] hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.388304] hns3_handle_bdinfo+0x 324/0x410 [hns3]		
			[ 5889.394055] hns3_handle_rx_bd+0x6 0/0x150 [hns3]		
			[ 5889.399624] hns3_clean_rx_ring+0x8 4/0x170 [hns3]		
			[ 5889.405270] hns3_nic_common_poll +0xa8/0x220 [hns3]		

0-1

1-2

2-3 3-4 4-5 Page 1007 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.411084] napi_poll+0xcc/0x264 [ 5889.415329] net_rx_action+0xd4/0x 21c		
			[ 5889.419911] do_softirq+0x130/0x 358		
			[ 5889.424484] irq_exit+0x134/0x154		
			[ 5889.428700] handle_domain_irq+0 x88/0xf0		
			[ 5889.433684] gic_handle_irq+0x78/0 x2c0		
			[ 5889.438319] el1_irq+0xb8/0x140		
			[ 5889.442354] arch_cpu_idle+0x18/0x 40		
			[ 5889.446816] default_idle_call+0x5c/ 0x1c0		
			[ 5889.451714] cpuidle_idle_call+0x174 /0x1b0		
			[ 5889.456692] do_idle+0xc8/0x160		
			[ 5889.460717] cpu_startup_entry+0x3 0/0xfc		
			[ 5889.465523] secondary_start_kernel +0x158/0x1ec		
			[ 5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80)		

0-1

1-2

2-3 3-4 4-5 Page 1008 of 1051 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
			[ 5889.477950] SMP: stopping secondary CPUs								
			[ 5890.514626] SMP: failed to stop secondary CPUs 0-69,71-95								
			[ 5890.522951] Starting crashdump kernel								
			CVE ID : CVE-2024- 26881								
			In the Linux kernel, the following vulnerability has been resolved:								
			block: fix deadlock between bd_link_disk_holder and partition scan	https://git.ke rnel.org/stabl e/c/03f12122							
		5.5	i						'open_mutex' of gendisk is used to protect open/close block devices. But	b20b6e6028e 9ed69030a49 f9cffcbb75, https://git.ke rnel.org/stabl	
Improper Locking	17-Apr-2024 5.5		in bd_link_disk_holder(), it is used to protect the creation of symlink	e/c/1e5c5b0a baee7b62a10 b9707a62083 b71ad21f62, https://git.ke rnel.org/stabl e/c/5a87c1f7 993bc8ac358	0-LIN-LINU- 030524/945						
			between holding disk and slave bdev, which introduces some issues.								
		When bd_link_disk_holder() is called, the driver is usually in the process	a3766bac5dc 7126e01e98								
			of initialization/modificati on and may suspend submitting io. At this								

0-1

1-2

2-3 3-4 4-5 Page 1009 of 1051 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			time, any io hold 'open_mutex', such as scanning partitions, can cause		
			deadlocks. For example, in raid:		
			T1 T2		
			bdev_open_by_dev		
			lock open_mutex [1]		
			···		
			efi_partition		
			md_submit_bio		
			md_ioctl mddev_syspend		
			-> suspend all io		
			md_add_new_disk		
			bind_rdev_to_array		
			bd_link_disk_holder		
			try lock open_mutex [2] md_handle_request		
			-> wait mddev_resume		
			T1 scan partition, T2 add a new device to		

0-1

1-2

2-33-44-5Page 1010 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			raid. T1 waits for T2 to resume		
			mddev, but T2 waits for open_mutex held by T1. Deadlock occurs.		
			Fix it by introducing a local mutex 'blk_holder_mutex' to replace		
			'open_mutex'.		
			CVE ID : CVE-2024- 26899		
			In the Linux kernel, the following vulnerability has been resolved:		
			do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak	https://git.ke rnel.org/stabl e/c/3948abaa	
			syzbot identified a kernel information leak vulnerability in	4e2be938ccdf c289385a273 42fb13d43, https://git.ke	
Use of Uninitialize d Resource	17-Apr-2024	5.5	do_sys_name_to_handle () and issued the following report [1].	rnel.org/stabl e/c/423b6bdf 19bbc5e1f7e7 46104509991	0-LIN-LINU- 030524/946
			[1]	7378f7e71, https://git.ke	
			"BUG: KMSAN: kernel- infoleak in instrument_copy_to_use	rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228	
			r include/linux/instrume nted.h:114 [inline]	a68d8a7c1	
			BUG: KMSAN: kernel- infoleak in		
			_copy_to_user+0xbc/0x		
			100 lib/usercopy.c:40		

0-1

1-2

2-33-44-5Page 1011 of 1051

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instrument_copy_to_use r include/linux/instrume nted.h:114 [inline]		
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40 copy_to_user include/linux/uaccess.h		
			:191 [inline] do_sys_name_to_handle fs/fhandle.c:73 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94 x64_sys_name_to_han		
			dle_at+0xe4/0x140 fs/fhandle.c:94 		
			Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517		

0-1

1-2

2-33-44-5Page 1012 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_kmalloc_node mm/slab_common.c:10 06 [inline]		
			_kmalloc+0x121/0x3c 0 mm/slab_common.c:10 20		
			kmalloc include/linux/slab.h:60 4 [inline]		
			do_sys_name_to_handle fs/fhandle.c:39 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Bytes 18-19 of 20 are uninitialized		
			Memory access of size 20 starts at ffff888128a46380		
			Data copied to user address 0000000020000240"		
			Per Chuck Lever's suggestion, use		

0-1

1-2

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kzalloc() instead of kmalloc() to		
			solve the problem.		
			CVE ID : CVE-2024- 26901		
			In the Linux kernel, the following vulnerability has been resolved:		
			perf: RISCV: Fix panic on pmu overflow handler		
NULL Pointer Dereferenc e	17-Apr-2024	5.5	<pre>(1 &lt;&lt; idx) of int is not desired when setting bits in unsigned long overflowed_ctrs, use BIT() instead. This panic happens when running 'perf record -e branches' on sophgo sg2042.</pre> [ 273.311852] Unable to handle kernel NULL pointer dereference at virtual address 000000000000098	https://git.ke rnel.org/stabl e/c/34b5678 68777e9fd39 ec533396972 8a7f0cf179c, https://git.ke rnel.org/stabl e/c/3ede8e94 de6b834b48b 0643385e663 63e7a04be9, https://git.ke rnel.org/stabl e/c/9f599ba3 b9cc4bdb8ec 1e3f0feddd41 bf9d296d6	O-LIN-LINU- 030524/947
			[ 273.320851] Oops [#1]	517027000	
			[ 273.323179] Modules linked in:		
			[ 273.326303] CPU: 0 PID: 1475 Comm: perf Not tainted 6.6.0-rc3+ #9		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 273.332521] Hardware name: Sophgo Mango (DT)		
			[ 273.336878] epc : riscv_pmu_ctr_get_widt h_mask+0x8/0x62		
			[ 273.342291] ra : pmu_sbi_ovf_handler+0 x2e0/0x34e		
			[ 273.347091] epc : ffffffff80aecd98 ra : ffffffff80aee056 sp : fffffff6e36928b0		
			[ 273.354454] gp : fffffff821f82d0 tp : ffffffd90c353200 t0 : 0000002ade4f9978		
			[ 273.361815] t1 : 0000000000504d55 t2 : fffffff8016cd8c s0 : fffffff6e3692a70		
			[ 273.369180] s1: 0000000000000020 a0 : 0000000000000000 a1: 00001a8e81800000		
			[ 273.376540] a2 : 0000003c00070198 a3 : 0000003c00db75a4 a4 : 00000000000000015		
			[ 273.383901] a5 : ffffffd7ff8804b0 a6 : 0000000000000015 a7 : 000000000000002a		
			[ 273.391327] s2 : 0000000000000ffff s3 : 00000000000000000 s4 : ffffffd7ff8803b0		
			[ 273.398773] s5 : 0000000000504d55 s6		

0-1

1-2

2-33-44-5Page 1015 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			: ffffffd905069800 s7 : fffffff821fe210		
			[ 273.406139] s8 : 000000007fffffff s9 : fffffd7ff8803b0 s10: ffffffd903f29098		
			[ 273.413660] s11: 0000000080000000 t3 : 0000000000000003 t4 : fffffff8017a0ca		
			[ 273.421022] t5 : ffffffff8023cfc2 t6 : ffffffd9040780e8		
			[ 273.426437] status: 0000000200000100 badaddr: 0000000000000098 cause: 00000000000000000d		
			[ 273.434512] [ <ffffffff80aecd98>] riscv_pmu_ctr_get_widt h_mask+0x8/0x62</ffffffff80aecd98>		
			[ 273.441169] [ <ffffffff80076bd8>] handle_percpu_devid_ir q+0x98/0x1ee</ffffffff80076bd8>		
			[ 273.447562] [ <ffffffff80071158>] generic_handle_domain _irq+0x28/0x36</ffffffff80071158>		
			[ 273.454151] [ <ffffffff8047a99a>] riscv_intc_irq+0x36/0x 4e</ffffffff8047a99a>		
			[ 273.459659] [ <fffffff80c944de>] handle_riscv_irq+0x4a/ 0x74</fffffff80c944de>		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 273.465442] [ <fffffff80c94c48>] do_irq+0x62/0x92</fffffff80c94c48>		
			[ 273.470360] Code: 0420 60a2 6402 5529 0141 8082 0013 0000 0013 0000 (6d5c) b783		
			[ 273.477921][ end trace 0000000000000000000000 ]		
			[ 273.482630] Kernel panic - not syncing: Fatal exception in interrupt		
			CVE ID : CVE-2024- 26902		
			In the Linux kernel, the following vulnerability has been resolved:		
			Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security	https://git.ke rnel.org/stabl e/c/2535b84 8fa0f42ddff3e 5255cf5e742c	
NULL Pointer Dereferenc	17-Apr-2024	5.5	During our fuzz testing of the connection and disconnection process at the	9b77bb26, https://git.ke rnel.org/stabl e/c/369f419c 097e82407dd	O-LIN-LINU- 030524/948
е			RFCOMM layer, we discovered this bug. By comparing the packets from a	429a202cde9 a73d3ae29b, https://git.ke rnel.org/stabl	
			normal connection and disconnection process with the testcase that	e/c/3ead59ba fad05f2967ae 2438c0528d5 3244cfde5	
			triggered a KASAN report. We analyzed the cause of this bug as follows:		

0-1

1-2

**2-3** 3-4 4-5 Page **1017** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1. In the packets captured during a normal connection, the host sends a		
			`Read Encryption Key Size` type of `HCI_CMD` packet		
			(Command Opcode: 0x1408) to the controller to inquire the length of		
			encryption key.After receiving this packet, the controller immediately		
			replies with a Command Completepacket (Event Code: 0x0e) to return the		
			Encryption Key Size.		
			2. In our fuzz test case, the timing of the controller's response to this		
			packet was delayed to an unexpected point: after the RFCOMM and L2CAP		
			layers had disconnected but before the HCI layer had disconnected.		
			3. After receiving the Encryption Key Size Response at the time described		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in point 2, the host still called the rfcomm_check_security function.		
			However, by this time `struct l2cap_conn *conn = l2cap_pi(sk)- >chan->conn;`		
			had already been released, and when the function executed		
			`return hci_conn_security(conn ->hcon, d->sec_level, auth_type, d->out);`,		
			specifically when accessing `conn->hcon`, a null-ptr-deref error occurred.		
			To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling		
			rfcomm_recv_frame in rfcomm_process_rx.		
			CVE ID : CVE-2024- 26903		
Improper Locking			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/2daa2a8e 895e6dc2395 f8628c011bcf 1e019040d,	
	17-Apr-2024	024 5.5	btrfs: fix data race at btrfs_use_block_rsv() when accessing block reserve	https://git.ke rnel.org/stabl e/c/7e9422d 35d574b6462 69ca46010a8 35ca074b310, https://git.ke	O-LIN-LINU- 030524/949

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			At btrfs_use_block_rsv() we read the size of a block reserve without	rnel.org/stabl e/c/ab1be3f1 aa7799f9915	
			locking its spinlock, which makes KCSAN complain because the size of a	5488c28eacae f65eb68fb	
			block reserve is always updated while holding its spinlock. The report		
			from KCSAN is the following:		
			[653.313148] BUG: KCSAN: data-race in btrfs_update_delayed_r efs_rsv [btrfs] / btrfs_use_block_rsv [btrfs]		
			[653.314755] read to 0x000000017f5871b8 of 8 bytes by task 7519 on cpu 0:		
			[653.314779] btrfs_use_block_rsv+0x e4/0x2f8 [btrfs]		
			[653.315606] btrfs_alloc_tree_block+0 xdc/0x998 [btrfs]		
			[653.316421] btrfs_force_cow_block+ 0x220/0xe38 [btrfs]		
			[653.317242] btrfs_cow_block+0x1ac /0x568 [btrfs]		
			[653.318060] btrfs_search_slot+0xda 2/0x19b8 [btrfs]		

0-1

1-2

2-33-44-5Page 1020 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.318879] btrfs_del_csums+0x1dc /0x798 [btrfs]		
			[653.319702] btrfs_free_extent.isra. 0+0xc24/0x2028 [btrfs]		
			[653.320538] btrfs_run_delayed_ref s+0xd3c/0x2390 [btrfs]		
			[653.321340] btrfs_run_delayed_refs+ 0xae/0x290 [btrfs]		
			[653.322140] flush_space+0x5e4/0x7 18 [btrfs]		
			[653.322958] btrfs_preempt_reclaim_ metadata_space+0x102 /0x2f8 [btrfs]		
			[653.323781] process_one_work+0x3 b6/0x838		
			[653.323800] worker_thread+0x75e/ 0xb10		
			[653.323817] kthread+0x21a/0x230		
			[653.323836] ret_from_fork+0x6c/0 xb8		
			[653.323855] ret_from_fork+0xa/0x3 0		
			[653.323887] write to 0x000000017f5871b8 of 8 bytes by task 576 on cpu 3:		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.323906] btrfs_update_delayed_r efs_rsv+0x1a4/0x250 [btrfs]		
			[653.324699] btrfs_add_delayed_data _ref+0x468/0x6d8 [btrfs]		
			[653.325494] btrfs_free_extent+0x76 /0x120 [btrfs]		
			[653.326280] btrfs_mod_ref+0x6a8/ 0x6b8 [btrfs]		
			[653.327064] btrfs_dec_ref+0x50/0x7 0 [btrfs]		
			[653.327849] walk_up_proc+0x236/0 xa50 [btrfs]		
			[653.328633] walk_up_tree+0x21c/0x 448 [btrfs]		
			[653.329418] btrfs_drop_snapshot+0x 802/0x1328 [btrfs]		
			[653.330205] btrfs_clean_one_deleted _snapshot+0x184/0x23 8 [btrfs]		
			[653.330995] cleaner_kthread+0x2b0 /0x2f0 [btrfs]		
			[653.331781] kthread+0x21a/0x230		
			[653.331800] ret_from_fork+0x6c/0 xb8		

0-1

1-2

2-33-44-5Page 1022 of 1051

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.331818] ret_from_fork+0xa/0x3 0		
			So add a helper to get the size of a block reserve while holding the lock.		
			Reading the field while holding the lock instead of using the data_race()		
			annotation is used in order to prevent load tearing.		
			CVE ID : CVE-2024- 26904		
			In the Linux kernel, the following vulnerability has been resolved:		
			soc: qcom: pmic_glink_altmode: fix drm bridge use-after- free	https://git.ke rnel.org/stabl e/c/2bbd65c 6ca567ed8db bfc4fb945f57 ce64bef342, https://git.ke	
Use After Free	17-Apr-2024	2024 5.5	A recent DRM series purporting to simplify support for "transparent	rnel.org/stabl e/c/b979f2d5 0a099f34024 18d7ff5f26c3	0-LIN-LINU- 030524/950
			bridges" and handling of probe deferrals ironically exposed a	952fb08bb, https://git.ke rnel.org/stabl e/c/ef45aa28	
			use-after-free issue on pmic_glink_altmode probe deferral.	41e15b649e5 417fe3d4de3 95fe462781	
			This has manifested itself as the display		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subsystem occasionally failing to initialise and NULL- pointer dereferences during boot of machines like		
			the Lenovo ThinkPad X13s.		
			Specifically, the dp-hpd bridge is currently registered before all		
			resources have been acquired which means that it can also be		
			deregistered on probe deferrals.		
			In the meantime there is a race window where the new aux bridge driver		
			(or PHY driver previously) may have looked up the dp-hpd bridge and		
			stored a (non- reference-counted) pointer to the bridge which is about to		
			be deallocated.		
			When the display controller is later initialised, this triggers a		
			use-after-free when attaching the bridges:		

0-1

1-2

2-3 3-4 4-5 Page **1024** of **1051**  6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dp -> aux -> dp- hpd (freed)		
			which may, for example, result in the freed bridge failing to attach:		
			[drm:drm_bridg e_attach [drm]] *ERROR* failed to attach bridge /soc@0/phy@88eb000 to encoder TMDS-31: - 16		
			or a NULL-pointer dereference:		
			Unable to handle kernel NULL pointer dereference at virtual address 00000000000000000		
			 Call trace:		
			drm_bridge_attach+0x7 0/0x1a8 [drm]		
			drm_aux_bridge_attach +0x24/0x38 [aux_bridge]		
			drm_bridge_attach+0x8 0/0x1a8 [drm]		
			dp_bridge_init+0xa8/0x 15c [msm]		

0-1

1-2

2-3 3-4 4-5 Page **1025** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			msm_dp_modeset_init+ 0x28/0xc4 [msm]		
			The DRM bridge implementation is clearly fragile and implicitly built on		
			the assumption that bridges may never go away. In this case, the fix is		
			to move the bridge registration in the pmic_glink_altmode driver to		
			after all resources have been looked up.		
			Incidentally, with the new dp-hpd bridge implementation, which registers		
			child devices, this is also a requirement due to a long-standing issue		
			in driver core that can otherwise lead to a probe deferral loop (see		
			commit fbc35b45f9f6 ("Add documentation on meaning of - EPROBE_DEFER")).		
			[DB: slightly fixed commit message by adding the word 'commit']		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024- 26909		
Affected Ver	sion(s): From (i	ncluding)	6.7 Up to (excluding) 6.7.6	)	
	Concurrent Execution using Shared Resource with 17-Apr-2024 4.7	ncluding)	In the Linux kernel, the following vulnerability has been resolved: pmdomain: mediatek: fix race conditions with genpd If the power domains are registered first with genpd and *after that* the driver attempts to power them on in the	https://git.ke rnel.org/stabl e/c/339ddc9 83bc1622341 d95f244c261c	
Execution using Shared Resource with Improper Synchroniz ation ('Race		-2024 4.7	probe sequence, then it is possible that a race condition occurs if genpd tries to power them on in the same time. The same is valid for powering them off before unregistering them from genpd.	d95f244c361c da3da3a4ff, https://git.ke rnel.org/stabl e/c/3cd1d92e e1dbf3e8f988 767eb75f262 07397792b, https://git.ke rnel.org/stabl e/c/475426a d1ae0bfdfd8f 160ed975090	0-LIN-LINU- 030524/951
		Attempt to fix race conditions by first removing the domains from genpd and *after that* powering down domains. Also first power up the domains and *after that* register them to genpd.	3799392438		

0-1

1-2

2-3 3-4 4-5 Page **1027** of **1051**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 52645		
			In the Linux kernel, the following vulnerability has been resolved:		
			netfilter: ipset: fix performance regression in swap operation		
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	17-Apr-2024	4.7	The patch "netfilter: ipset: fix race condition between swap/destroy and kernel side add/del/test", commit 28628fa9 fixes a race condition. But the synchronize_rcu() added to the swap function unnecessarily slows it down: it can safely be moved to destroy and use call_rcu() instead. Eric Dumazet pointed out that simply calling the destroy functions as rcu callback does not work: sets with timeout use garbage collectors which need cancelling at destroy which can wait. Therefore the	https://git.ke rnel.org/stabl e/c/653bc5e6 d9995d7d5f4 97c665b3218 75a626161c, https://git.ke rnel.org/stabl e/c/970709a 67696b100a5 7b33af1a3d7 5fc34b747eb, https://git.ke rnel.org/stabl e/c/97f7cf1cd 80eeed3b7c8 08b7c124632 95c751001	O-LIN-LINU- 030524/952
		destroy functions are split into two: cancelling garbage collectors safely at			

0-1

1-2

2-3 3-4 4-5 Page **1028** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executing the command received by netlink and moving the remaining		
			part only into the rcu callback.		
			CVE ID : CVE-2024- 26910		
Affected Ver	<mark>sion(s): From (</mark> i	ncluding)	6.8 Up to (excluding) 6.8.2		
			In the Linux kernel, the following vulnerability has been resolved:		
	17-Apr-2024 7.8		net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv()	https://git.ke rnel.org/stabl	
			Apply the same fix than ones found in :	e/c/5c03387 021cfa3336b 97e0dcba380	
N/A		7.8	8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in ip6_tnl_rcv()")	29917a8af2a, https://git.ke rnel.org/stabl e/c/60044ab 84836359534	0-LIN-LINU- 030524/953
			1ca1ba465e55 ("geneve: make sure to pull inner header in geneve_rx()")	bd7153b92e9 c1584140e4a, https://git.ke rnel.org/stabl e/c/77fd5294	
			We have to save skb- >network_header in a temporary variable	ea09b21f677 2ac954a121b 87323cec80	
			in order to be able to recompute the network_header pointer		
			after a pskb_inet_may_pull() call.		

0-1

1-2

2-3 3-4 4-5 Page **1029** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pskb_inet_may_pull() makes sure the needed headers are in skb- >head.		
			syzbot reported: BUG: KMSAN: uninit- value in INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			BUG: KMSAN: uninit- value in INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			BUG: KMSAN: uninit- value in IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		
			BUG: KMSAN: uninit- value in ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40		
			9 INET_ECN_decapsulat e include/net/inet_ecn.h: 253 [inline]		
			INET_ECN_decapsulate include/net/inet_ecn.h: 275 [inline]		
			IP_ECN_decapsulate include/net/inet_ecn.h: 302 [inline]		

0-1

1-2

2-33-44-5Page 1030 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_tunnel_rcv+0xed9/0 x2ed0 net/ipv4/ip_tunnel.c:40 9		
			ipgre_rcv+0x9bc/0xb c0 net/ipv4/ip_gre.c:389		
			ipgre_rcv net/ipv4/ip_gre.c:411 [inline]		
			gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447		
			gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c: 163		
			ip_protocol_deliver_rcu +0x264/0x1300 net/ipv4/ip_input.c:205		
			ip_local_deliver_finish+ 0x2b8/0x440 net/ipv4/ip_input.c:233		
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_local_deliver+0x21f/ 0x490 net/ipv4/ip_input.c:254		
			dst_input include/net/dst.h:461 [inline]		
			ip_rcv_finish net/ipv4/ip_input.c:449 [inline]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NF_HOOK include/linux/netfilter. h:314 [inline]		
			ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569		
			netif_receive_skb_one _core net/core/dev.c:5534 [inline]		
			netif_receive_skb+0x1 a6/0x5a0 net/core/dev.c:5648		
			netif_receive_skb_intern al net/core/dev.c:5734 [inline]		
			netif_receive_skb+0x58 /0x660 net/core/dev.c:5793		
			tun_rx_batched+0x3ee/ 0x980 drivers/net/tun.c:1556		
			tun_get_user+0x53b9/0 x66e0 drivers/net/tun.c:2009		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		

0-1

1-2

2-33-44-5Page 1032 of 1051

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b		
			Uninit was created at:		
			alloc_pages+0x9a6/0x e00 mm/page_alloc.c:4590		
			alloc_pages_mpol+0x62 b/0x9d0 mm/mempolicy.c:2133		
			alloc_pages+0x1be/0x1		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e0 mm/mempolicy.c:2204		
			skb_page_frag_refill+0x 2bf/0x7c0 net/core/sock.c:2909		
			tun_build_skb drivers/net/tun.c:1686 [inline]		
			tun_get_user+0xe0a/0x 66e0 drivers/net/tun.c:1826		
			tun_chr_write_iter+0x3 af/0x5d0 drivers/net/tun.c:2055		
			call_write_iter include/linux/fs.h:2087 [inline]		
			new_sync_write fs/read_write.c:497 [inline]		
			vfs_write+0xb6b/0x15 20 fs/read_write.c:590		
			ksys_write+0x20f/0x4c 0 fs/read_write.c:643		
			do_sys_write fs/read_write.c:655 [inline]		
			se_sys_write fs/read_write.c:652 [inline]		
			x64_sys_write+0x93/ 0xd0 fs/read_write.c:652		

0-1

1-2

2-3 3-4 4-5 Page **1034** of **1051**  5-6

6-7

 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/comm on.c:52 [inline]		
			do_syscall_64+0xcf/0x1 e0 arch/x86/entry/comm on.c:83		
			entry_SYSCALL_64_afte r_hwframe+0x63/0x6b <b>CVE ID : CVE-2024-</b>		
			26882		
			In the Linux kernel, the following vulnerability has been resolved:		
			bpf: Fix stackmap overflow check on 32- bit arches	https://git.ke rnel.org/stabl e/c/0971126	
Improper Restriction of			The stackmap code relies on roundup_pow_of_two() to compute the number	c8164abe200 4b8536b4969 0a0d6005b0a, https://git.ke rnel.org/stabl e/c/1564100 7df0f0d35fa2 8742b25c2a7 db9dcd6895, https://git.ke rnel.org/stabl e/c/21e5fa46	
Operations within the Bounds of	17-Apr-2024	17-Apr-2024 7.8	of hash buckets, and contains an overflow check by checking if the		0-LIN-LINU- 030524/954
a Memory Buffer			resulting value is 0. However, on 32-bit arches, the roundup code itself		
			can overflow by doing a 32-bit left-shift of an unsigned long value,	88e1a4d3db6 b72216231b2 4232f75c1d	
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on		

0-1

1-2

2-33-44-5Page 1035 of 1051

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code.		
			The commit in the fixes tag actually attempted to fix this, but the fix		
			did not account for the UB, so the fix only works on CPUs where an		
			overflow does result in a neat truncation to zero, which is not		
			guaranteed. Checking the value before rounding does not have this		
			problem.		
			CVE ID : CVE-2024- 26883		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/33ec04ca db77605b71d	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2024 7.8		bpf: Fix hashtab overflow check on 32- bit arches	92983119193 03d390c4d5, https://git.ke rnel.org/stabl e/c/3b08cfc6	O-LIN-LINU-
		7.8	The hashtab code relies on roundup_pow_of_two() to compute the number	5f07b1132c1 979d73f014a e6e04de55d, https://git.ke rnel.org/stabl	030524/955
			of hash buckets, and contains an overflow check by checking if the	e/c/64f00b4d f0597590b19 9b62a37a165 473bf658a6	

0-1

1-2

2-3 3-4 4-5 Page **1036** of **1051**  5-6

6-7

 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting value is 0. However, on 32-bit arches, the roundup code itself		
			can overflow by doing a 32-bit left-shift of an unsigned long value,		
			which is undefined behaviour, so it is not guaranteed to truncate		
			neatly. This was triggered by syzbot on the DEVMAP_HASH type, which		
			contains the same check, copied from the hashtab code. So apply the same		
			fix to hashtab, by moving the overflow check to before the roundup.		
			CVE ID : CVE-2024- 26884		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/22079b3	
Improper Restriction of	Restriction		bpf: Fix DEVMAP_HASH overflow check on 32- bit arches	a423382335f 47d9ed32114 e6c9fe88d7c, https://git.ke	
Operations within the Bounds of a Memory Buffer	17-Apr-2024	7.8	The devmap code allocates a number hash buckets equal to the next power	rnel.org/stabl e/c/225da02 acdc97af01b6 bc6ce1a3e53 62bf01d3fb, https://git.ke	O-LIN-LINU- 030524/956
			of two of the max_entries value provided when creating the map. When	rnel.org/stabl e/c/250051ac c21f9d4c5c59	

0-1

1-2

2-3 3-4 4-5 Page **1037** of **1051**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rounding up to the next power of two, the 32-bit variable storing the	5e4fcb55986e a08c4691	
			number of buckets can overflow, and the code checks for overflow by		
			checking if the truncated 32-bit value is equal to 0. However, on 32-bit		
			arches the rounding up itself can overflow mid- way through, because it		
			ends up doing a left- shift of 32 bits on an unsigned long value. If the		
			size of an unsigned long is four bytes, this is undefined behaviour, so		
			there is no guarantee that we'll end up with a nice and tidy 0-value at		
			the end.		
			Syzbot managed to turn this into a crash on arm32 by creating a DEVMAP_HASH with max_entries > 0x80000000 and then		
			trying to update it. Fix this by moving the overflow check to before the rounding up		
			operation.		
			CVE ID : CVE-2024- 26885		

0-1

1-2

2-3 3-4 4-5 Page **1038** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE IDIn the Linux kernel, the following vulnerability has been resolved:aoe: fix the potential use-after-free problem in aoecmd_cfg_pktsThis patch is against CVE-2023-6270. The description of cve is:A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on	https://git.ke rnel.org/stabl e/c/079cba4f 4e307c69878 226fdf5228c2 0aa1c969c, https://git.ke rnel.org/stabl e/c/1a54aa50 6b3b2f31496	NCIIPC ID
			`struct net_device`, and a use-after-free can be triggered by racing between the free on the struct and the access through the `skbtxq` global queue. This could lead to a denial of service condition or potential code execution. In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial	731039e4977 8f54eee881, https://git.ke rnel.org/stabl e/c/74ca3ef6 8d2f449bc84 8c0a814cefc4 87bf755fa	

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code is finished. But the net_device ifp will still be used in		
			later tx()- >dev_queue_xmit() in kthread. Which means that the		
			dev_put(ifp) should NOT be called in the success path of skb		
			initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into		
			use-after-free because the net_device is freed.		
			This patch removed the dev_put(ifp) in the success path in		
			aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx().		
			CVE ID : CVE-2024- 26898		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/0fbcf236 6ba9888cf02e da23e35fde7f	
NULL Pointer Dereferenc e	17-Apr-2024	5.5	net: hns3: fix kernel crash when 1588 is received on HIP08 devices	7fcc07c3, https://git.ke rnel.org/stabl e/c/11b9983 60d96f6c76f0 4a95f54b49f2	0-LIN-LINU- 030524/958
			The HIP08 devices does not register the ptp devices, so the	4d3c858e4, https://git.ke rnel.org/stabl e/c/23ec1cec 24293f9799c	

0-1

1-2

2-3 3-4 4-5 Page **1040** of **1051**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hdev->ptp is NULL, but the hardware can receive 1588 messages,	725941677d4 e167997265	
			and set the HNS3_RXD_TS_VLD_B bit, so, if match this case, the		
			access of hdev->ptp- >flags will cause a kernel crash:		
			[ 5888.946472] Unable to handle kernel NULL pointer dereference at virtual address 000000000000018		
			[ 5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 00000000000018		
			 [ 5889.266118] pc : hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.272612] lr : hclge_ptp_get_rx_hwts+ 0x34/0x170 [hclge]		
			[ 5889.279101] sp : ffff800012c3bc50		
			[ 5889.283516] x29: ffff800012c3bc50 x28: ffff2040002be040		
			[ 5889.289927] x27: ffff800009116484 x26: 0000000080007500		
			[ 5889.296333] x25: 00000000000000000 x24: ffff204001c6f000		

0-1

1-2

2-3 3-4 4-5 Page **1041** of **1051**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.302738] x23: ffff204144f53c00 x22: 00000000000000000		
			[ 5889.309134] x21: 0000000000000000 x20: ffff204004220080		
			[ 5889.315520] x19: ffff204144f53c00 x18: 00000000000000000		
			[ 5889.321897] x17: 00000000000000000 x16:		
			0000000000000000 [ 5889.328263] x15: 0000004000140ec8 x14: 00000000000000000000000		
			[ 5889.334617] x13: 00000000000000000 x12: 00000000010011df		
			[ 5889.340965] x11: bbfeff4d22000000 x10: 000000000000000000		
			[ 5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d		
			[ 5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480		
			[ 5889.359959] x5 : 0000000000000000 x4 : 000000000000000000		
			[ 5889.366271] x3 : 000000000000000 x2 : 00000000000000000		
			[ 5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.378857] Call trace:		
			[ 5889.382285] hclge_ptp_get_rx_hwts+ 0x40/0x170 [hclge]		
			[ 5889.388304] hns3_handle_bdinfo+0x 324/0x410 [hns3]		
			[ 5889.394055] hns3_handle_rx_bd+0x6 0/0x150 [hns3]		
			[ 5889.399624] hns3_clean_rx_ring+0x8 4/0x170 [hns3]		
			[ 5889.405270] hns3_nic_common_poll +0xa8/0x220 [hns3]		
			[ 5889.411084] napi_poll+0xcc/0x264		
			[ 5889.415329] net_rx_action+0xd4/0x 21c		
			[ 5889.419911] do_softirq+0x130/0x 358		
			[ 5889.424484] irq_exit+0x134/0x154		
			[ 5889.428700] handle_domain_irq+0 x88/0xf0		
			[ 5889.433684] gic_handle_irq+0x78/0 x2c0		
			[ 5889.438319] el1_irq+0xb8/0x140		
			[ 5889.442354] arch_cpu_idle+0x18/0x 40		

0-1

1-2

2-3 3-4 4-5 Page **1043** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[ 5889.446816] default_idle_call+0x5c/ 0x1c0		
			[ 5889.451714] cpuidle_idle_call+0x174 /0x1b0		
			[ 5889.456692] do_idle+0xc8/0x160		
			[ 5889.460717] cpu_startup_entry+0x3 0/0xfc		
			[ 5889.465523] secondary_start_kernel +0x158/0x1ec		
			[ 5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80)		
			[ 5889.477950] SMP: stopping secondary CPUs		
			[ 5890.514626] SMP: failed to stop secondary CPUs 0-69,71-95		
			[ 5890.522951] Starting crashdump kernel		
			CVE ID : CVE-2024- 26881		
			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/03f12122 b20b6e6028e 9ed69030a49	
Improper Locking	17-Apr-2024	5.5	block: fix deadlock between bd_link_disk_holder and partition scan	f9cffcbb75, https://git.ke rnel.org/stabl e/c/1e5c5b0a baee7b62a10	0-LIN-LINU- 030524/959
			'open_mutex' of gendisk is used to protect	b9707a62083 b71ad21f62, https://git.ke	

0-1

1-2

5-6

6-7

open/close block       mel.org/stabl         devices. But       in         in       bd_link_disk_holder(), it         is used to protect the       creation of symlink         between holding disk       and slave bdev, which         introduces some issues.       When         bd_link_disk_holder() is       called, the driver is         usually in the process       of         initialization/modificati       on and may suspend         submitting io. At this       time, any io hold         'open_mutex', such as       scanning partitions, can         cause       deadlocks. For example,         In raid:       T1       T2         bdev_open_by_dev       lock open_mutex [1]          ef_partition          md_submit_bio	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
and slave bdev, which         introduces some issues.         When         bd_link_disk_holder() is         called, the driver is         usually in the process         of         initialization/modificati         on and may suspend         submitting io. At this         time, any io hold         'open_mutex', such as         scanning partitions, can         cause         deadlocks. For example,         in raid:         T1       T2         bdev_open_by_dev         lock open_mutex [1]            efi_partition				devices. But in bd_link_disk_holder(), it is used to protect the creation of symlink	e/c/5a87c1f7 993bc8ac358 a3766bac5dc	
of initialization/modificati on and may suspend submitting io. At this time, any io hold 'open_mutex', such as scanning partitions, can cause deadlocks. For example, in raid: T1 T2 bdev_open_by_dev lock open_mutex [1]  efi_partition 				introduces some issues. When bd_link_disk_holder() is called, the driver is		
scanning partitions, can cause deadlocks. For example, in raid: T1 T2 bdev_open_by_dev lock open_mutex [1]  efi_partition 				of initialization/modificati on and may suspend submitting io. At this		
bdev_open_by_dev lock open_mutex [1]  efi_partition 				scanning partitions, can cause deadlocks. For example,		
 efi_partition 						
md_submit_bio						
md_ioctl						
mddev_syspend -> suspend all io				mddev_syspend -> suspend all		

0-1

1-2

2-3 3-4 4-5 Page **1045** of **1051**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			md_add_new_disk		
			bind_rdev_to_array		
			bd_link_disk_holder		
			try lock open_mutex [2]		
			md_handle_request -> wait mddev_resume		
			T1 scan partition, T2 add a new device to raid. T1 waits for T2 to resume		
			mddev, but T2 waits for open_mutex held by T1. Deadlock occurs.		
			Fix it by introducing a local mutex 'blk_holder_mutex' to replace		
			'open_mutex'. CVE ID : CVE-2024- 26899		
Missing Release of Memory			In the Linux kernel, the following vulnerability has been resolved:	https://git.ke rnel.org/stabl e/c/4c1021ce 46fc2fb6115f	O-LIN-LINU-
after Effective Lifetime	17-Apr-2024	pr-2024 5.5	md: fix kmemleak of rdev->serial	7e79d353941 e6dcad366, https://git.ke rnel.org/stabl e/c/6cf35065	030524/960

0-1

1-2

2-3 3-4 4-5 Page **1046** of **1051**  5-6

6-7

8-9

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If kobject_add() is fail in bind_rdev_to_array(), 'rdev->serial' will be	8736681b9d6 b0b6e58c5c7 6b235bb4c4,	
			alloc not be freed, and kmemleak occurs.	https://git.ke rnel.org/stabl e/c/6d32c83	
			unreferenced object 0xffff88815a350000 (size 49152):	2a88513f65c 2c2c9c75954 ee8b387adea	
			comm "mdadm", pid 789, jiffies 4294716910		
			hex dump (first 32 bytes):		
			00 00 00 00 00 00 00 00 00 00 00 00 00 0		
			00 00 00 00 00 00 00 00 00 00 00 00 00 0		
			backtrace (crc f773277a):		
			[<0000000058b0a453> ]		
			kmemleak_alloc+0x61/ 0xe0		
			[<00000000366adf14> ]		
			kmalloc_large_node+0 x15e/0x270		
			[<000000002e82961b> ]		
			kmalloc_node.cold+0x 11/0x7f		
			[<00000000f206d60a> ]		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kvmalloc_node+0x74/0 x150		
			[<0000000034bf3363> ]		
			rdev_init_serial+0x67/0 x170		
			[<0000000010e08fe9>] mddev_create_serial_po ol+0x62/0x220		
			[<00000000c3837bf0>] bind_rdev_to_array+0x 2af/0x630		
			[<0000000073c28560>		
			nd_add_new_disk+0x4 00/0x9f0		
			[<00000000770e30ff>] md_ioctl+0x15bf/0x1c1 0		
			[<000000006cfab718>] blkdev_ioctl+0x191/0x 3f0		
			[<0000000085086a11> ] vfs_ioctl+0x22/0x60		
			[<0000000018b656fe>		
			] x64_sys_ioctl+0xba/0 xe0		
			[<00000000e54e675e> ]		
			do_syscall_64+0x71/0x 150		

0-1

1-2

2-3 3-4 4-5 Page **1048** of **1051**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<pre>[&lt;00000008b0ad622&gt; ] entry_SYSCALL_64_afte r_hwframe+0x6c/0x74 CVE ID : CVE-2024- 26900</pre>		
Use of Uninitialize d Resource	17-Apr-2024	5.5	26900 In the Linux kernel, the following vulnerability has been resolved: do_sys_name_to_handle (): use kzalloc() to fix kernel-infoleak syzbot identified a kernel information leak vulnerability in do_sys_name_to_handle () and issued the following report [1]. [1] "BUG: KMSAN: kernel- infoleak in instrument_copy_to_use r include/linux/instrume nted.h:114 [inline] BUG: KMSAN: kernel- infoleak in _copy_to_user+0xbc/0x 100 lib/usercopy.c:40	https://git.ke rnel.org/stabl e/c/3948abaa 4e2be938ccdf c289385a273 42fb13d43, https://git.ke rnel.org/stabl e/c/423b6bdf 19bbc5e1f7e7 46104509991 7378f7e71, https://git.ke rnel.org/stabl e/c/4bac28f4 41e3cc9d3f1a 84c8d023228 a68d8a7c1	O-LIN-LINU- 030524/961
			instrument_copy_to_use r include/linux/instrume nted.h:114 [inline]		

0-1

1-2

2-3 3-4 4-5 Page **1049** of **1051**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_copy_to_user+0xbc/0x 100 lib/usercopy.c:40		
			copy_to_user include/linux/uaccess.h :191 [inline]		
			do_sys_name_to_handle fs/fhandle.c:73 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x949/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Uninit was created at:		
			slab_post_alloc_hook+0 x129/0xa70 mm/slab.h:768		
			slab_alloc_node mm/slub.c:3478 [inline]		
			kmem_cache_alloc_no de+0x5c9/0x970 mm/slub.c:3517		
			do_kmalloc_node mm/slab_common.c:10 06 [inline]		
			_kmalloc+0x121/0x3c 0		

0-1

1-2

2-33-44-5Page 1050 of 1051

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/slab_common.c:10 20		
			kmalloc include/linux/slab.h:60 4 [inline]		
			do_sys_name_to_handle fs/fhandle.c:39 [inline]		
			do_sys_name_to_hand le_at fs/fhandle.c:112 [inline]		
			se_sys_name_to_handl e_at+0x441/0xb10 fs/fhandle.c:94		
			x64_sys_name_to_han dle_at+0xe4/0x140 fs/fhandle.c:94		
			Bytes 18-19 of 20 are uninitialized		
			Memory access of size 20 starts at ffff888128a46380		
			Data copied to user address 0000000020000240"		
			Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to		
			solve the problem.		
			CVE ID : CVE-2024- 26901		

0-1

1-2

6-7 7-8

5-6