National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 30 Apr 2024 Vol. 11 No. 8

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: aditya88					
Product: online_furniture_shopping_ecommerce_website					
Affected Version(s): 1.0					
Improper Neutralization 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. **CVE ID : CVE-2024-4071**	N/A	A-ADI-ONLI-030524/1
Improper Neutralization 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

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. **CVE ID : CVE-2024-4072**		
Vendor: Cisco					
Product: firepower_threat_defense					
Affected Version(s): 6.2.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/3

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/4

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 Version(s): 6.2.3.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 6.2.3.10					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/8

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 6.2.3.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/10

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.12					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/11

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/12

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 Version(s): 6.2.3.13					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/13

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/14

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.14					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/15

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/16

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.15					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/17

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/18

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.16					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/19

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/20

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 Version(s): 6.2.3.17					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/21

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/22

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.18					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/23

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/24

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 Version(s): 6.2.3.2					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 6.2.3.3					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/28

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 6.2.3.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/30

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.5					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/31

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/32

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 Version(s): 6.2.3.6					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/33

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/34

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.7					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/35

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/36

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.8					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/37

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/38

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.2.3.9					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/39

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/40

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 Version(s): 6.4.0					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/41

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/42

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/43

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/44

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 Version(s): 6.4.0.10					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 6.4.0.11					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/48

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 6.4.0.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/50

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.13					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/51

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/52

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 Version(s): 6.4.0.14					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/53

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/54

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.15					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/55

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/56

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.16					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/57

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/58

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.17					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/59

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/60

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 Version(s): 6.4.0.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/61

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/62

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/63

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/64

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 Version(s): 6.4.0.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 6.4.0.5					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/68

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 6.4.0.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/70

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.7					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/71

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/72

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 Version(s): 6.4.0.8					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/73

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/74

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.4.0.9					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/75

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/76

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.6.0					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/77

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/78

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.6.0.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/79

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/80

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 Version(s): 6.6.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/81

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/82

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.6.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/83

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/84

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 Version(s): 6.6.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 6.6.5					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/88

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 6.6.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/90

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.6.5.2					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/91

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/92

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 Version(s): 6.6.7					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/93

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/94

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.6.7.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/95

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/96

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.7.0					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/97

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/98

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.7.0.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/99

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/100

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 Version(s): 6.7.0.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/101

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/102

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 6.7.0.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/103

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/104

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 Version(s): 7.0.0					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 7.0.0.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/108

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 7.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/110

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.0.1.1					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/111

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/112

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 Version(s): 7.0.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/113

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/114

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.0.2.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/115

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/116

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.0.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/117

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/118

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.0.4					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/119

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/120

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 Version(s): 7.0.5					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/121

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/122

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.0.6					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/123

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/124

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 Version(s): 7.0.6.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 7.1.0					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/128

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 7.1.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/130

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.1.0.2					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/131

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/132

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 Version(s): 7.1.0.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/133

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/134

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.2.0					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/135

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/136

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.2.0.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/137

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/138

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.2.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/139

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/140

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 Version(s): 7.2.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/141

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/142

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.2.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/143

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/144

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 Version(s): 7.2.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security	A-CIS-FIRE-030524/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			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 (SIR) of this advisory from Medium to High.	/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20359		
Affected Version(s): 7.2.4.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/148

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. 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**	persist-rce-FLsNXF4h	
Affected Version(s): 7.2.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/150

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.2.5.1					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-FIRE-030524/151

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. 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**	ityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/152

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 Version(s): 7.3.0					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/153

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. **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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/154

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.3.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/155

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. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/156

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.3.1.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/157

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/158

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 7.4.0					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/159

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/160

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 Version(s): 7.4.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	A-CIS-FIRE-030524/161

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	A-CIS-FIRE-030524/162

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. **CVE ID : CVE-2024-20359**		
Product: firepower_threat_defense_software					
Affected Version(s): 6.2.3					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/163

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 Version(s): 6.2.3.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system as root. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.2.3.10					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Affected Version(s): 6.2.3.11					
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/166
Affected Version(s): 6.2.3.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/167
Affected Version(s): 6.2.3.13					
Improper Neutralization of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-FIRE-030524/168

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. **CVE ID : CVE-2024-20358**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	
Affected Version(s): 6.2.3.14					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/169

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. **CVE ID : CVE-2024-20358**	cmd-inj-ZJV8Wysm	
Affected Version(s): 6.2.3.15					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/170

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.2.3.16					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/171

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.2.3.17					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/172

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 Version(s): 6.2.3.18					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/173

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 Version(s): 6.2.3.2					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/174

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.2.3.3					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/175

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 Version(s): 6.2.3.4					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Affected Version(s): 6.2.3.5					
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/177
Affected Version(s): 6.2.3.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/178
Affected Version(s): 6.2.3.7					
Improper Neutralization of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-FIRE-030524/179

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. **CVE ID : CVE-2024-20358**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	
Affected Version(s): 6.2.3.8					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/180

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. **CVE ID : CVE-2024-20358**	cmd-inj-ZJV8Wysm	
Affected Version(s): 6.2.3.9					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/181

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.4.0					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/182

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.4.0.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/183

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 Version(s): 6.4.0.10					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/184

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 Version(s): 6.4.0.11					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/185

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.4.0.12					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/186

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 Version(s): 6.4.0.13					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Affected Version(s): 6.4.0.14					
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/188
Affected Version(s): 6.4.0.15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/189
Affected Version(s): 6.4.0.16					
Improper Neutralization of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-FIRE-030524/190

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. **CVE ID : CVE-2024-20358**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	
Affected Version(s): 6.4.0.17					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/191

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. **CVE ID : CVE-2024-20358**	cmd-inj-ZJV8Wysm	
Affected Version(s): 6.4.0.2					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/192

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.4.0.3					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/193

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.4.0.4					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/194

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 Version(s): 6.4.0.5					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/195

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 Version(s): 6.4.0.6					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/196

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.4.0.7					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/197

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 Version(s): 6.4.0.8					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Affected Version(s): 6.4.0.9					
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/199
Affected Version(s): 6.6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/200
Affected Version(s): 6.6.0.1					
Improper Neutralization of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-FIRE-030524/201

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. **CVE ID : CVE-2024-20358**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	
Affected Version(s): 6.6.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/202

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. **CVE ID : CVE-2024-20358**	cmd-inj-ZJV8Wysm	
Affected Version(s): 6.6.3					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/203

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.6.4					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/204

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.6.5					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/205

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 Version(s): 6.6.5.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/206

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 Version(s): 6.6.5.2					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/207

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 6.6.7					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/208

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 Version(s): 6.6.7.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Affected Version(s): 6.7.0					
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/210
Affected Version(s): 6.7.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/211
Affected Version(s): 6.7.0.2					
Improper Neutralization of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-FIRE-030524/212

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. **CVE ID : CVE-2024-20358**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	
Affected Version(s): 6.7.0.3					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/213

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. **CVE ID : CVE-2024-20358**	cmd-inj-ZJV8Wysm	
Affected Version(s): 7.0.0					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/214

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.0.0.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/215

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.0.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/216

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 Version(s): 7.0.1.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/217

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 Version(s): 7.0.2					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/218

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.0.2.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/219

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 Version(s): 7.0.3					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Affected Version(s): 7.0.4					
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/221
Affected Version(s): 7.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/222
Affected Version(s): 7.0.6					
Improper Neutralization of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-FIRE-030524/223

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. **CVE ID : CVE-2024-20358**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	
Affected Version(s): 7.0.6.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/224

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. **CVE ID : CVE-2024-20358**	cmd-inj-ZJV8Wysm	
Affected Version(s): 7.1.0					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/225

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.1.0.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/226

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.1.0.2					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/227

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 Version(s): 7.1.0.3					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/228

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 Version(s): 7.2.0					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/229

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.2.0.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/230

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 Version(s): 7.2.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Affected Version(s): 7.2.2					
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/232
Affected Version(s): 7.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/233
Affected Version(s): 7.2.4					
Improper Neutralization of Special	24-Apr-2024	6.7	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-FIRE-030524/234

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. **CVE ID : CVE-2024-20358**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	
Affected Version(s): 7.2.4.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	A-CIS-FIRE-030524/235

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. **CVE ID : CVE-2024-20358**	cmd-inj-ZJV8Wysm	
Affected Version(s): 7.2.5					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/236

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.2.5.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/237

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.3.0					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/238

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 Version(s): 7.3.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/239

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 Version(s): 7.3.1.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/240

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. **CVE ID : CVE-2024-20358**		
Affected Version(s): 7.4.0					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/241

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 Version(s): 7.4.1					
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	A-CIS-FIRE-030524/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20358		
Vendor: crushftp					
Product: crushftp					
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.7.1					
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. **CVE ID : CVE-2024-4040**	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/1c850i2/all_versions_of_crush_ftp_are_vulnerable/	A-CRU-CRUS-030524/243
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.1.0					
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/1c850i2/all_versions_of_crus	A-CRU-CRUS-030524/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-4040	h_ftp_are_vulnerable/	
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 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) **CVE ID : CVE-2024-3834**	https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html	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://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html	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://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html	A-GOO-CHRO-030524/247

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) **CVE ID : CVE-2024-3838**	https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html	A-GOO-CHRO-030524/248
Vendor: IBM					
Product: aspera_faspex					
Affected Version(s): From (including) 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. **CVE ID : CVE-2023-27279**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248533, https://www.ibm.com/support/pages/node/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. **CVE ID : CVE-2022-40745**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236452, https://www.ibm.com/support/pages/node/7148632	A-IBM-ASPE-030524/250

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. **CVE ID : CVE-2023-37397**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259672, https://www.ibm.com/support/pages/node/7148632	A-IBM-ASPE-030524/251
Vendor: Oracle					
Product: complex_maintenance_repair_and_overhaul					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.13					
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/security-alerts/cpuapr2024.html	A-ORA-COMP-030524/252

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/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-21026**		
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	https://www.oracle.com/security-alerts/cpuapr2024.html	A-ORA-COMP-030524/253

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. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-21027**		
N/A	16-Apr-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product	https://www.oracle.com/security-	A-ORA-COMP-030524/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 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	alerts/cpuapr2024.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR: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/security-alerts/cpuapr2024.html	A-ORA-COMP-030524/255

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/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-21029**		
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/security-alerts/cpuapr2024.html	A-ORA-COMP-030524/256

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/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-21030**		
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/security-alerts/cpuapr2024.html	A-ORA-COMP-030524/257

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/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-21031**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operating System					
Vendor: Cisco					
Product: adaptive_security_appliance_software					
Affected Version(s): 9.12.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/258
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/259

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/260

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.1.2					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/261

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/262

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/263

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.1.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/264

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/265

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/266

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/267

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/268

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/269

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 Version(s): 9.12.2.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/272

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.12.2.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/273
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/274

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/275

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.2.5					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/276

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/277

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/278

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 Version(s): 9.12.2.9					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/279

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/280

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/281

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 Version(s): 9.12.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/283

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.3.12					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/285
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/286

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/287

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.3.2					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/288

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/289

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/290

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.3.7					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/291

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/292

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/293

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.3.9					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/294

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/295

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/296

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 Version(s): 9.12.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/299

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.12.4.10					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/300
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/301

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/302

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.13					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/303

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/304

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/305

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 Version(s): 9.12.4.18					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/306

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/307

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/308

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 Version(s): 9.12.4.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/310

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.24					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/312
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/313

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/314

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.26					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/315

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/316

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/317

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.29					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/318

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/319

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/320

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.30					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/321

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/322

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/323

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 Version(s): 9.12.4.35					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/326

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.12.4.37					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/327
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/328

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/329

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.38					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/330

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/331

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/332

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 Version(s): 9.12.4.39					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/333

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/334

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/335

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 Version(s): 9.12.4.4					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/337

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.40					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/339
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/340

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/341

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.41					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/342

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/343

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/344

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.47					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/345

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/346

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/347

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.48					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/348

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/349

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/350

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 Version(s): 9.12.4.50					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/353

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.12.4.52					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/354
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/355

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/356

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.54					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/357

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/358

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/359

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 Version(s): 9.12.4.55					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/360

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/361

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/362

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 Version(s): 9.12.4.56					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/364

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.58					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/366
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/367

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/368

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.62					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/369

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/370

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/371

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.65					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/372

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/373

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/374

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.12.4.7					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/375

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/376

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/377

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 Version(s): 9.12.4.8					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/380

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.14.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/381
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/382

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/383

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.1.10					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/384

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/385

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/386

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 Version(s): 9.14.1.15					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/387

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/388

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/389

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 Version(s): 9.14.1.19					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/391

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.1.30					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/393
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/394

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/395

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.1.6					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/396

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/397

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/398

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/399

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/400

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/401

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.2.13					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/402

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/403

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/404

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 Version(s): 9.14.2.15					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/407

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.14.2.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/408
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/409

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/410

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.2.8					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/411

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/412

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/413

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 Version(s): 9.14.3					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/414

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/415

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/416

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 Version(s): 9.14.3.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/418

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.3.11					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/420
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/421

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/422

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.3.13					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/423

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/424

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/425

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.3.15					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/426

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/427

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/428

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.3.18					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/429

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/430

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/431

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 Version(s): 9.14.3.9					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/434

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.14.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/435
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/436

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/437

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.4.12					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/438

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/439

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/440

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 Version(s): 9.14.4.13					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/441

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/442

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/443

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 Version(s): 9.14.4.14					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/445

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.4.15					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/447
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/448

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/449

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.4.17					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/450

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/451

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/452

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.4.22					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/453

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/454

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/455

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.14.4.23					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/456

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/457

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/458

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 Version(s): 9.14.4.6					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/461

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.14.4.7					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/462
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/463

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/464

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.15.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/465

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/466

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/467

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 Version(s): 9.15.1.1					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/468

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/469

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/470

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 Version(s): 9.15.1.10					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/472

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.15.1.15					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/474
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/475

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/476

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.15.1.16					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/477

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/478

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/479

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.15.1.17					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/480

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/481

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/482

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.15.1.21					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/483

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/484

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/485

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 Version(s): 9.15.1.7					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/488

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.16.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/489
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/490

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/491

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.1.28					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/492

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/493

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/494

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 Version(s): 9.16.2					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/495

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/496

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/497

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 Version(s): 9.16.2.11					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/499

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.2.13					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/501
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/502

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/503

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.2.14					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/504

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/505

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/506

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.2.3					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/507

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/508

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/509

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.2.7					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/510

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/511

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/512

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 Version(s): 9.16.3					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/515

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.16.3.14					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/516
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/517

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/518

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.3.15					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/519

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/520

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/521

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 Version(s): 9.16.3.19					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/522

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/523

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/524

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 Version(s): 9.16.3.23					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/526

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.3.3					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/528
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/529

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/530

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.4					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/531

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/532

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/533

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.4.14					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/534

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/535

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/536

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.4.18					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/537

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/538

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/539

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 Version(s): 9.16.4.19					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/542

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.16.4.27					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/543
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/544

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/545

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.4.38					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/546

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/547

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/548

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 Version(s): 9.16.4.39					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/549

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/550

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/551

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 Version(s): 9.16.4.42					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/553

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.4.48					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/555
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/556

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/557

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.4.55					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/558

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/559

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/560

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.16.4.9					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/561

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/562

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/563

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.17.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/564

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/565

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/566

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 Version(s): 9.17.1.10					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/569

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.17.1.11					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/570
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/571

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/572

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.17.1.13					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/573

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/574

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/575

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 Version(s): 9.17.1.15					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/576

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/577

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/578

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 Version(s): 9.17.1.20					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/580

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.17.1.30					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/582
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/583

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/584

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.17.1.33					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/585

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/586

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/587

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.17.1.7					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/588

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/589

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/590

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.17.1.9					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/591

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/592

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/593

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 Version(s): 9.18.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/596

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.18.1.3					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/597
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/598

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/599

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.18.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/600

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/601

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/602

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 Version(s): 9.18.2.5					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/603

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/604

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/605

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 Version(s): 9.18.2.7					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/607

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.18.2.8					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/609
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/610

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/611

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.18.3					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/612

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/613

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/614

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.18.3.39					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/615

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/616

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/617

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.18.3.46					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/618

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/619

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/620

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 Version(s): 9.18.3.53					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/623

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.18.3.55					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/624
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/625

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/626

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.18.3.56					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/627

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/628

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/629

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 Version(s): 9.18.4					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/630

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/631

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/632

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 Version(s): 9.18.4.5					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/634

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.18.4.8					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/636
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/637

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/638

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.19.1					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/639

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/640

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/641

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.19.1.12					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/642

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/643

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/644

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.19.1.18					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/645

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/646

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/647

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 Version(s): 9.19.1.22					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/650

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.19.1.24					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/651
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/652

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/653

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.19.1.27					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/654

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/655

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/656

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 Version(s): 9.19.1.5					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/657

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/658

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/659

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 Version(s): 9.19.1.9					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/661

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.20.1					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/663
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/664

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/665

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.20.1.5					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/666

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/667

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/668

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.20.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/669

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/670

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/671

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.1					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/672

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/673

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/674

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 Version(s): 9.8.1.5					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/677

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.1.7					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/678
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/679

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/680

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.2					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/681

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/682

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/683

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 Version(s): 9.8.2.14					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/684

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/685

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/686

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 Version(s): 9.8.2.15					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/688

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.2.17					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/690
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/691

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/692

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.2.20					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/693

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/694

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/695

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.2.24					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/696

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/697

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/698

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.2.26					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/699

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/700

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/701

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 Version(s): 9.8.2.28					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/704

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.2.33					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/705
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/706

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/707

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.2.35					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/708

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/709

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/710

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 Version(s): 9.8.2.38					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/711

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/712

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/713

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 Version(s): 9.8.2.8					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/715

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.3					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/717
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/718

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/719

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.3.11					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/720

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/721

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/722

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.3.14					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/723

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/724

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/725

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.3.16					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/726

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/727

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/728

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 Version(s): 9.8.3.18					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/731

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.3.21					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/732
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/733

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/734

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.3.26					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/735

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/736

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/737

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 Version(s): 9.8.3.29					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/738

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/739

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/740

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 Version(s): 9.8.3.8					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/742

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/744
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/745

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/746

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.10					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/747

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/748

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/749

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.12					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/750

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/751

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/752

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.15					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/753

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/754

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/755

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 Version(s): 9.8.4.17					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/758

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.4.20					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/759
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/760

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/761

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.22					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/762

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/763

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/764

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 Version(s): 9.8.4.25					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/765

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/766

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/767

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 Version(s): 9.8.4.26					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/769

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.29					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/771
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/772

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/773

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.3					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/774

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/775

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/776

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.32					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/777

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/778

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/779

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.33					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/780

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/781

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/782

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 Version(s): 9.8.4.34					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/785

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.4.35					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/786
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/787

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/788

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.39					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/789

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/790

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/791

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 Version(s): 9.8.4.40					
Loop with Unreachable 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/792

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. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/793

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/794

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 Version(s): 9.8.4.41					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition when the device reloads. **CVE ID : CVE-2024-20353**		
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/796

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SIR) of this advisory from Medium to High. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.43					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/798
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/799

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. **CVE ID : CVE-2024-20358**	ityAdvisory/cisco-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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/800

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.44					
Loop with Unreachable Exit Condition	24-Apr-2024	8.6	A vulnerability in the management and VPN web servers for Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ADAP-030524/801

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. 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**	nt/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/802

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. **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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/803

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.45					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/804

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/805

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**		
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/806

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.46					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/807

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 Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/808

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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/809

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 Version(s): 9.8.4.48					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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. **CVE ID : CVE-2024-20358**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-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.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-ADAP-030524/812

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. 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**	ityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.8.4.7					
Loop with Unreachable 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. **CVE ID : CVE-2024-20353**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2	O-CIS-ADAP-030524/813
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/814

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/815

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. **CVE ID : CVE-2024-20359**		
Affected Version(s): 9.8.4.8					
Loop with Unreachable 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	O-CIS-ADAP-030524/816

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. 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**	websrvs-dos-X8gNucD2	
Improper Neutralization 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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm	O-CIS-ADAP-030524/817

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. **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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h	O-CIS-ADAP-030524/818

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**		
Product: ios_xe					
Affected Version(s): 17.10.1					
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/819

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. **CVE ID : CVE-2024-20313**		
Affected Version(s): 17.10.1a					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/820
Affected Version(s): 17.10.1b					
Buffer Copy	24-Apr-2024	7.4	A vulnerability in the OSPF version 2	https://sec.cloudapps.cisco	O-CIS-IOS_-030524/821

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. **CVE ID : CVE-2024-20313**	.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	
Affected Version(s): 17.11.1					
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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/822

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. **CVE ID : CVE-2024-20313**		
Affected Version(s): 17.11.1a					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/823
Affected Version(s): 17.11.99sw					

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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/824
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/825

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. **CVE ID : CVE-2024-20313**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20313		
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/827
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/828

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 Version(s): 17.6.1w					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2024-20313**		
Affected Version(s): 17.6.1x					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/830
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-	O-CIS-IOS_-030524/831

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. **CVE ID : CVE-2024-20313**	ospf-dos-dR9Sfrxp	
Affected Version(s): 17.6.1z					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/832

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 Version(s): 17.6.1z1					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/833
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	O-CIS-IOS_-030524/834

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. **CVE ID : CVE-2024-20313**	sco-sa-iosxe-ospf-dos-dR9Sfrxp	
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/835

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 Version(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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/836
Affected Version(s): 17.6.4					
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.cloudapps.cisco.com/security/center/conte	O-CIS-IOS_-030524/837

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. **CVE ID : CVE-2024-20313**	nt/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/838

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. **CVE ID : CVE-2024-20313**		
Affected Version(s): 17.6.5a					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/839
Affected Version(s): 17.7.1					
Buffer Copy	24-Apr-2024	7.4	A vulnerability in the OSPF version 2	https://sec.cloudapps.cisco	O-CIS-IOS_-030524/840

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. **CVE ID : CVE-2024-20313**	.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/841

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. **CVE ID : CVE-2024-20313**		
Affected Version(s): 17.7.1b					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/842
Affected Version(s): 17.7.2					

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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/843
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/844

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. **CVE ID : CVE-2024-20313**		
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20313		
Affected Version(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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/846
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/847

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 Version(s): 17.9.1w					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reload, resulting in a DoS condition. **CVE ID : CVE-2024-20313**		
Affected Version(s): 17.9.1x					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/849
Affected Version(s): 17.9.1x1					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-	O-CIS-IOS_-030524/850

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. **CVE ID : CVE-2024-20313**	ospf-dos-dR9Sfrxp	
Affected Version(s): 17.9.1y					
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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/851

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 Version(s): 17.9.1y1					
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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/852
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	O-CIS-IOS_-030524/853

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. **CVE ID : CVE-2024-20313**	sco-sa-iosxe-ospf-dos-dR9Sfrxp	
Affected Version(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.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-CIS-IOS_-030524/854

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 Version(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. **CVE ID : CVE-2024-20313**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	O-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.cloudapps.cisco.com/security/center/conte	O-CIS-IOS_-030524/856

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. **CVE ID : CVE-2024-20313**	nt/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp	
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 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.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/15641007df0f0d35fa28742b25c2a7db9dcd6895, https://git.kernel.org/stable/c/21e5fa46	O-LIN-LINU-030524/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 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**	88e1a4d3db6b72216231b24232f75c1d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Apr-2024	5.5	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 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	https://git.kernel.org/stable/c/2535b848fa0f42ddff3e5255cf5e742c9b77bb26, https://git.kernel.org/stable/c/369f419c097e82407dd429a202cde9a73d3ae29b, https://git.kernel.org/stable/c/3ead59bafad05f2967ae2438c0528d53244cfde5	O-LIN-LINU-030524/858

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`,		

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 Version(s): * Up to (excluding) 5.10.214					
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while accessing Eth segment ------------[cut here]------------ memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 (size 2) WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131	https://git.kernel.org/stable/c/185fa07000e0a81d54cf8c05414cebff14469a5c, https://git.kernel.org/stable/c/4d5e86a56615cc387d21c629f9af8fb0e958d350, https://git.kernel.org/stable/c/60ba938a8bc8c90e724c75f98e932f9fb7ae1b9d	O-LIN-LINU-030524/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mlx5_ib_post_send+0x191b/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 ghash_clmulni_intel sha512_ssse3 snd_pcsp aesni_intel crypto_simd		

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_send+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: 0000000000000000 RBX: 0000000000000001		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffb5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80 FS: 00007fc03b444c80(0000) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? show_regs+0x72/0x90 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0 ? handle_bug+0x46/0x90 ? exc_invalid_op+0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_send_nodrain+0xb/0x20 [mlx5_ib] ipoib_send+0x2ec/0x770 [ib_ipoib]		

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 ? __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		

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+0x64/0x70 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0 tcp_write_xmit+0x334/0x8d0 tcp_push_one+0x3c/0x60 tcp_sendmsg_locked+0x2e1/0xac0 tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sock_write_iter+0x93/0x100 vfs_write+0x326/0x3c0 ksys_write+0xbd/0xf0 ? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_ ---truncated--- **CVE ID : CVE-2024-26907**		
Affected Version(s): * Up to (excluding) 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.kernel.org/stable/c/1f08a1b26cfc53b7715abc46857c6023bb1b87de, https://git.kernel.org/stable/c/8e65edf0d37698f7a6cb174608d3ec7976baf49e, https://git.kernel.org/stable/c/e9076ffbcaed5da6c182b144ef9f6e24554af268	O-LIN-LINU-030524/860

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 Version(s): * Up to (excluding) 5.4.269					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix performance regression in swap operation 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	https://git.kernel.org/stable/c/653bc5e6d9995d7d5f497c665b321875a626161c, https://git.kernel.org/stable/c/970709a67696b100a57b33af1a3d75fc34b747eb, https://git.kernel.org/stable/c/97f7cf1cd80eeed3b7c808b7c12463295c751001	O-LIN-LINU-030524/861

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 Version(s): * Up to (excluding) 5.4.273					
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	https://git.kernel.org/stable/c/2daa2a8e895e6dc2395f8628c011bcf1e019040d, https://git.kernel.org/stable/c/7e9422d35d574b646269ca46010a835ca074b310, https://git.kernel.org/stable/c/ab1be3f1aa7799f99155488c28eacaef65eb68fb	O-LIN-LINU-030524/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			btrfs_update_delayed_refs_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+0xe4/0x2f8 [btrfs] [653.315606] btrfs_alloc_tree_block+0xdc/0x998 [btrfs] [653.316421] btrfs_force_cow_block+0x220/0xe38 [btrfs] [653.317242] btrfs_cow_block+0x1ac/0x568 [btrfs] [653.318060] btrfs_search_slot+0xda2/0x19b8 [btrfs] [653.318879] btrfs_del_csums+0x1dc/0x798 [btrfs] [653.319702] __btrfs_free_extent.isra.0+0xc24/0x2028 [btrfs] [653.320538] __btrfs_run_delayed_refs+0xd3c/0x2390 [btrfs] [653.321340] btrfs_run_delayed_refs+0xae/0x290 [btrfs] [653.322140] flush_space+0x5e4/0x718 [btrfs]		

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+0x3b6/0x838 [653.323800] worker_thread+0x75e/0xb10 [653.323817] kthread+0x21a/0x230 [653.323836] __ret_from_fork+0x6c/0xb8 [653.323855] ret_from_fork+0xa/0x30 [653.323887] write to 0x000000017f5871b8 of 8 bytes by task 576 on cpu 3: [653.323906] btrfs_update_delayed_refs_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+0x50/0x70 [btrfs]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.327849] walk_up_proc+0x236/0xa50 [btrfs] [653.328633] walk_up_tree+0x21c/0x448 [btrfs] [653.329418] btrfs_drop_snapshot+0x802/0x1328 [btrfs] [653.330205] btrfs_clean_one_deleted_snapshot+0x184/0x238 [btrfs] [653.330995] cleaner_kthread+0x2b0/0x2f0 [btrfs] [653.331781] kthread+0x21a/0x230 [653.331800] __ret_from_fork+0x6c/0xb8 [653.331818] ret_from_fork+0xa/0x30 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 Version(s): * Up to (excluding) 6.6.23					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Apr-2024	5.5	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 0000000000000098 [273.320851] Oops [#1] [273.323179] Modules linked in: [273.326303] CPU: 0 PID: 1475 Comm: perf Not tainted 6.6.0-rc3+ #9 [273.332521] Hardware name: Sophgo Mango (DT) [273.336878] epc : riscv_pmu_ctr_get_width_mask+0x8/0x62	https://git.kernel.org/stable/c/34b567868777e9fd39ec5333969728a7f0cf179c, https://git.kernel.org/stable/c/3ede8e94de6b834b48b0643385e66363e7a04be9, https://git.kernel.org/stable/c/9f599ba3b9cc4bdb8ec1e3f0fedd41bf9d296d6	O-LIN-LINU-030524/863

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 : ffffffff821f82d0 tp : ffffffd90c353200 t0 : 0000002ade4f9978 [273.361815] t1 : 0000000000504d55 t2 : ffffffff8016cd8c s0 : ffffffff6e3692a70 [273.369180] s1 : 0000000000000020 a0 : 0000000000000000 a1 : 00001a8e81800000 [273.376540] a2 : 0000003c00070198 a3 : 0000003c00db75a4 a4 : 0000000000000015 [273.383901] a5 : ffffffd7ff8804b0 a6 : 0000000000000015 a7 : 000000000000002a [273.391327] s2 : 000000000000ffff s3 : 0000000000000000 s4 : ffffffd7ff8803b0 [273.398773] s5 : 0000000000504d55 s6 : ffffffd905069800 s7 : ffffffff821fe210 [273.406139] s8 : 00000007ffffff s9 : ffffffd7ff8803b0 s10: ffffffd903f29098		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[273.413660] s11: 0000000080000000 t3 : 0000000000000003 t4 : ffffffff8017a0ca [273.421022] t5 : ffffffff8023cfc2 t6 : ffffffd9040780e8 [273.426437] status: 0000000200000100 badaddr: 0000000000000098 cause: 000000000000000d [273.434512] [<ffffffff80aecd98>] riscv_pmu_ctr_get_width_mask+0x8/0x62 [273.441169] [<ffffffff80076bd8>] handle_percpu_devid_irq+0x98/0x1ee [273.447562] [<ffffffff80071158>] generic_handle_domain_irq+0x28/0x36 [273.454151] [<ffffffff8047a99a>] riscv_intc_irq+0x36/0x4e [273.459659] [<ffffffff80c944de>] handle_riscv_irq+0x4a/0x74 [273.465442] [<ffffffff80c94c48>] do_irq+0x62/0x92 [273.470360] Code: 0420 60a2 6402 5529 0141 8082 0013 0000 0013 0000 (6d5c) b783		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[273.477921] ---[end trace 0000000000000000]--- [273.482630] Kernel panic - not syncing: Fatal exception in interrupt **CVE ID : CVE-2024-26902**		
Affected Version(s): * Up to (excluding) 6.7.6					
Integer Underflow (Wrap or Wraparound)	17-Apr-2024	7.8	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. **CVE ID : CVE-2024-26913**	https://git.kernel.org/stable/c/cdbe0be8874c63bca85b8c38e5b1eecbdd18df31, https://git.kernel.org/stable/c/faf51b201bc42adf500945732abb6220c707d6f3	O-LIN-LINU-030524/864
Affected Version(s): From (excluding) 5.15 Up to (excluding) 5.15.71					
N/A	28-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/61703b248be993eb4997b00ae5d33	O-LIN-LINU-030524/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. 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-	18e6d8f3c5b, https://git.kernel.org/stable/c/df6cb39335cf5a1b918e8dbd8ba7cd9f1d00e45a, https://git.kernel.org/stable/c/e45cc288724f0cfd497bb5920bcfa60caa335729	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wq:nvme_delete_ctrl_work [nvme_core] is flushing !WQ_MEM_RECLAIM events:flush_cpu_slab WARNING: CPU: 37 PID: 410 at kernel/workqueue.c:2637 check_flush_dependency+0x10a/0x120 Workqueue: nvme-delete-wq nvme_delete_ctrl_work [nvme_core] RIP: 0010:check_flush_dependency+0x10a/0x120[453.262125] Call Trace: __flush_work.isra.0+0xbf/0x220 ? __queue_work+0x1dc/0x420 flush_all_cpus_locked+0xfb/0x120 __kmem_cache_shutdown+0x2b/0x320 kmem_cache_destroy+0x49/0x100 bioset_exit+0x143/0x190		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blk_release_queue+0xb9/0x100 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 Version(s): From (excluding) 5.16 Up to (excluding) 5.19.12					
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	https://git.kernel.org/stable/c/1f08a1b26cfc53b7715abc46857c6023bb1b87de, https://git.kernel.org/stable/c/8e65edf0d37698f7a6cb174608d3ec7976baf49e, https://git.kernel.org/stable/c/e9076ffbcaed5da6c182b144ef9f6e24554af268	O-LIN-LINU-030524/866

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.kernel.org/stable/c/61703b248be993eb4997b00ae5d3318e6d8f3c5b, https://git.kernel.org/stable/c/df6cb39335cf5a1b918e8dbd8ba7cd9f1d00e45a, https://git.kernel.org/stable/c/e45cc288724f0cfd497bb5920bcfa60caa335729	O-LIN-LINU-030524/867

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_work [nvme_core] is flushing !WQ_MEM_RECLAIM events:flush_cpu_slab WARNING: CPU: 37 PID: 410 at kernel/workqueue.c:2637 check_flush_dependency+0x10a/0x120 Workqueue: nvme-delete-wq nvme_delete_ctrl_work [nvme_core] RIP: 0010:check_flush_dependency+0x10a/0x120[453.262125] Call Trace: __flush_work.isra.0+0xbf/0x220		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __queue_work+0x1dc/0x420 flush_all_cpus_locked+0xfb/0x120 __kmem_cache_shutdown+0x2b/0x320 kmem_cache_destroy+0x49/0x100 bioset_exit+0x143/0x190 blk_release_queue+0xb9/0x100 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 Version(s): From (excluding) 6.7.0 Up to (excluding) 6.7.6					
Missing Release of Memory	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/042b5f83	O-LIN-LINU-030524/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			drm/nouveau: fix several DMA buffer leaks Nouveau manages GSP-RM DMA buffers with nvkm_gsp_mem objects. Several of 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	841fbf7ce39474412db3b5e4765a7ea7, https://git.kernel.org/stable/c/6190d4c08897d748dd25f0b78267a90aa1694e15	

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 Exceptional 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.kernel.org/stable/c/4b59c3fada06e5e8010ef7700689c71986e667a2, https://git.kernel.org/stable/c/8746c6c9dfa31d269c65dd52ab42fde0720b7d91	O-LIN-LINU-030524/869

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					
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem 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 potential code execution. In aoecmd_cfg_pkts(), it always calls	https://git.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c20aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc848c0a814cefc487bf755fa	O-LIN-LINU-030524/870

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 Version(s): From (including) 2.6.22 Up to (excluding) 4.9.330					
N/A	28-Apr-2024	5.5	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	https://git.kernel.org/stable/c/016b150992eebc32c4a18f783cf2bb6e2545a3d9, https://git.kernel.org/stable/c/02bcd951aa3c2cea95fb241c20802e9501940296,	O-LIN-LINU-030524/871

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(); 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:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335 kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0	https://git.kernel.org/stable/c/2d6e55e0c03804e1e227b80a5746e086d6c6696c	

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+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 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+0x2f8/0x408 fs/namespace.c:3568 **CVE ID : CVE-2022-48659**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.6.39 Up to (excluding) 4.19.311					
Use of Uninitialized 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_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 lib/usercopy.c:40 copy_to_user include/linux/uaccess.h:191 [inline]	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a27342fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991737 8f7e71, https://git.kernel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	O-LIN-LINU-030524/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_handle fs/fhandle.c:73 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_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 Version(s): From (including) 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: net: ip_tunnel: make sure to pull inner	https://git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a,	O-LIN-LINU-030524/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") 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_decapsulate include/net/inet_ecn.h:253 [inline]	https://git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a, https://git.kernel.org/stable/c/77fd5294ea09b21f6772ac954a121b87323cec80	

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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __ipgre_rcv+0x9bc/0xbc0 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		

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+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_intern		

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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055		

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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b **CVE ID : CVE-2024-26882**		
Affected Version(s): From (including) 3.19 Up to (excluding) 4.19.311					
Improper Restriction of Operations	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/33ec04cadb77605b71d	O-LIN-LINU-030524/874

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 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. **CVE ID : CVE-2024-26884**	92983119193 03d390c4d5, https://git.kernel.org/stable/c/3b08cfc65f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.295					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	28-Apr-2024	5.5	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 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:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335	https://git.kernel.org/stable/c/016b150992eebc32c4a18f783cf2bb6e2545a3d9, https://git.kernel.org/stable/c/02bcd951aa3c2cea95fb241c20802e9501940296, https://git.kernel.org/stable/c/2d6e55e0c03804e1e227b80a5746e086d6c6696c	O-LIN-LINU-030524/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0x78/0xb4 fs/f2fs/xattr.c:808 f2fs_fill_super+0x1050/0x1e0c fs/f2fs/super.c:4149 mount_bdev+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 fs/namespace.c:3370 do_mount fs/namespace.c:3383 [inline]		

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+0x2f8/0x408 fs/namespace.c:3568 **CVE ID : CVE-2022-48659**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.260					
N/A	28-Apr-2024	5.5	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 Call trace:	https://git.kernel.org/stable/c/016b150992eebc32c4a18f783cf2bb6e2545a3d9, https://git.kernel.org/stable/c/02bcd951aa3c2cea95fb241c20802e9501940296, https://git.kernel.org/stable/c/2d6e55e0c03804e1e227b80a5746e086d6c6696c	O-LIN-LINU-030524/876

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:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335 kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0x78/0xb4 fs/f2fs/xattr.c:808 f2fs_fill_super+0x1050/0x1e0c fs/f2fs/super.c:4149 mount_bdev+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 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+0x2f8/0x408 fs/namespace.c:3568 **CVE ID : CVE-2022-48659**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.215					
N/A	28-Apr-2024	5.5	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	https://git.kernel.org/stable/c/016b150992eebc32c4a18f783cf2bb6e2545a3d9, https://git.kernel.org/stable/c/02bcd951aa3c2cea95fb241c20802e9501940296, https://git.kernel.org/stabl	O-LIN-LINU-030524/877

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(); 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:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335 kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0	e/c/2d6e55e0c03804e1e227b80a5746e086d6c6696c	

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+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 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+0x2f8/0x408 fs/namespace.c:3568 **CVE ID : CVE-2022-48659**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 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.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/1564100 7df0f0d35fa28742b25c2a7db9dcd6895, https://git.kernel.org/stable/c/21e5fa4688e1a4d3db6b72216231b24232f75c1d	O-LIN-LINU-030524/878

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**		
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 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	https://git.kernel.org/stable/c/33ec04cadb77605b71d9298311919303d390c4d5, https://git.kernel.org/stable/c/3b08cfc65f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	O-LIN-LINU-030524/879

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**		
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem 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	https://git.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c20aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc848c0a814cefc487bf755fa	O-LIN-LINU-030524/880

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**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized 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_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 lib/usercopy.c:40 copy_to_user include/linux/uaccess.h:191 [inline] do_sys_name_to_handle fs/fhandle.c:73 [inline]	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a27342fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991737 8f7e71, https://git.kernel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	O-LIN-LINU-030524/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_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 Dereference	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security	https://git.kernel.org/stable/c/2535b848fa0f42ddff3e5255cf5e742c9b77bb26, https://git.kernel.org/stable/c/369f419c097e82407dd	O-LIN-LINU-030524/882

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 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	429a202cde9a73d3ae29b, https://git.kernel.org/stable/c/3ead59bafad05f2967ae2438c0528d53244cfde5	

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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26903		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.149					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix performance regression in swap operation 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 destroy	https://git.kernel.org/stable/c/653bc5e6d9995d7d5f497c665b321875a626161c, https://git.kernel.org/stable/c/970709a67696b100a57b33af1a3d75fc34b747eb, https://git.kernel.org/stable/c/97f7cf1cd80eeed3b7c808b7c12463295c751001	O-LIN-LINU-030524/883

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 Version(s): From (including) 5.11 Up to (excluding) 5.15.150					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	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 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. Attempt to fix race conditions by first	https://git.kernel.org/stable/c/339ddc983bc1622341d95f244c361cda3da3a4ff, https://git.kernel.org/stable/c/3cd1d92ee1dbf3e8f988767eb75f26207397792b, https://git.kernel.org/stable/c/475426ad1ae0bfdfd8f160ed9750903799392438	O-LIN-LINU-030524/884

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 Version(s): From (including) 5.11 Up to (excluding) 5.15.153					
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") 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	https://git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a, https://git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a, https://git.kernel.org/stable/c/77fd5294ea09b21f6772ac954a121b87323cec80	O-LIN-LINU-030524/885

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_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate include/net/inet_ecn.h:253 [inline]		

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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __ipgre_rcv+0x9bc/0xbc0 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		

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+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_internal 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+0x53b9/0x66e0 drivers/net/tun.c:2009 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055		

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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 fs/read_write.c:643 __do_sys_write fs/read_write.c:655 [inline]		

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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b **CVE ID : CVE-2024-26882**		
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	https://git.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/15641007df0f0d35fa28742b25c2a7db9dcd6895, https://git.kernel.org/stable/c/21e5fa4688e1a4d3db6b72216231b24232f75c1d	O-LIN-LINU-030524/886

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 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	https://git.kernel.org/stable/c/33ec04cadb77605b71d9298311919303d390c4d5, https://git.kernel.org/stable/c/3b08cfc6	O-LIN-LINU-030524/887

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 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**	5f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	
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	https://git.kernel.org/stable/c/22079b3a423382335f47d9ed32114e6c9fe88d7c, https://git.kernel.org/stable/c/225da02	O-LIN-LINU-030524/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 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.	acdc97af01b6bc6ce1a3e5362bf01d3fb, https://git.kernel.org/stable/c/250051acc21f9d4c5c595e4fcb55986ea08c4691	

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**		
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem 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 potential code execution.	https://git.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c20aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc848c0a814cefc487bf755fa	O-LIN-LINU-030524/889

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**		
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while accessing Eth segment ----------[cut here]----------	https://git.kernel.org/stable/c/185fa07000e0a81d54cf8c05414cebff14469a5c, https://git.kernel.org/stable/c/4d5e86a56615cc387d21c629f9af8fb0e958d350,	O-LIN-LINU-030524/890

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/drivers/infiniband/hw/mlx5/wr.c:131 (size 2) WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 mlx5_ib_post_send+0x191b/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	https://git.kernel.org/stable/c/60ba938a8bc8c90e724c75f98e932f9fb7ae1b9d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 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		

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: 0000000000000000 RBX: 0000000000000001 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffb5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80 FS: 00007fc03b444c80(00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? show_regs+0x72/0x90 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? handle_bug+0x46/0x90 ? exc_invalid_op+0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_send_nodrain+0xb/0x20 [mlx5_ib] ipoib_send+0x2ec/0x770 [ib_ipoib] ipoib_start_xmit+0x5a0/0x770 [ib_ipoib] dev_hard_start_xmit+0x8e/0x1e0 ? validate_xmit_skb_list+0x4d/0x80 sch_direct_xmit+0x116/0x3a0 __dev_xmit_skb+0x1fd/0x580 __dev_queue_xmit+0x284/0x6b0 ? _raw_spin_unlock_irq+0xe/0x50		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __flush_work.isra.0+0x20d/0x370 ? push_pseudo_header+0x17/0x40 [ib_ipoib] neigh_connected_output+0xcd/0x110 ip_finish_output2+0x179/0x480 ? __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+0x64/0x70 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_write_xmit+0x334/0x8d0 tcp_push_one+0x3c/0x60 tcp_sendmsg_locked+0x2e1/0xac0 tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80 sock_write_iter+0x93/0x100 vfs_write+0x326/0x3c0 ksys_write+0xbd/0xf0 ? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_ ---truncated--- **CVE ID : CVE-2024-26907**		
Use of Uninitialized Resource	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a273	O-LIN-LINU-030524/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 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_handle_at fs/fhandle.c:112 [inline]	42fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991 7378f7e71, https://git.kernel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_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 Dereference	17-Apr-2024	5.5	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.kernel.org/stable/c/2535b848fa0f42ddff3e5255cf5e742c9b77bb26, https://git.kernel.org/stable/c/369f419c097e82407dd429a202cde9a73d3ae29b, https://git.kernel.org/stabl	O-LIN-LINU-030524/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 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:	e/c/3ead59bafad05f2967ae2438c0528d53244cfde5	

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 Version(s): From (including) 5.11 Up to (excluding) 5.15.71					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	28-Apr-2024	5.5	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 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:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335	https://git.kernel.org/stable/c/016b150992eebc32c4a18f783cf2bb6e2545a3d9, https://git.kernel.org/stable/c/02bcd951aa3c2cea95fb241c20802e9501940296, https://git.kernel.org/stable/c/2d6e55e0c03804e1e227b80a5746e086d6c6696c	O-LIN-LINU-030524/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0x78/0xb4 fs/f2fs/xattr.c:808 f2fs_fill_super+0x1050/0x1e0c fs/f2fs/super.c:4149 mount_bdev+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 fs/namespace.c:3370 do_mount fs/namespace.c:3383 [inline]		

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+0x2f8/0x408 fs/namespace.c:3568 **CVE ID : CVE-2022-48659**		
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 gpiomon --num-events=3 --rising-edge gpiochip1 25 There will be a warning trace as below: Call trace: free_irq+0x204/0x360 lineevent_free+0x64/0x70 gpio_ioctl+0x598/0x6a0 __arm64_sys_ioctl+0xb4/0x100	https://git.kernel.org/stable/c/657803b918e097e47d99d1489da83a603c36bcdd, https://git.kernel.org/stable/c/69bef19d6b9700e96285f4b4e28691cda3dcd0d1, https://git.kernel.org/stable/c/97da736cd11ae73bdf2f5e21e24446b8349e0168	O-LIN-LINU-030524/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoke_syscall+0x5c/0x130 ..... el0t_64_sync+0x1a0/0x1a4 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 Version(s): From (including) 5.14 Up to (excluding) 5.15.153					
NULL Pointer Dereference	17-Apr-2024	5.5	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	https://git.kernel.org/stable/c/0fbcf2366ba9888cf02eda23e35fde7f7fcc07c3, https://git.kernel.org/stable/c/11b998360d96f6c76f04a95f54b49f24d3c858e4, https://git.kernel.org/stable/c/23ec1cec	O-LIN-LINU-030524/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 0000000000000018 [5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [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	24293f9799c725941677d4e167997265	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5889.302738] x23: ffff204144f53c00 x22: 0000000000000000 [5889.309134] x21: 0000000000000000 x20: ffff204004220080 [5889.315520] x19: ffff204144f53c00 x18: 0000000000000000 [5889.321897] x17: 0000000000000000 x16: 0000000000000000 [5889.328263] x15: 0000004000140ec8 x14: 0000000000000000 [5889.334617] x13: 0000000000000000 x12: 00000000010011df [5889.340965] x11: bbfeff4d22000000 x10: 0000000000000000 [5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d [5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480 [5889.359959] x5 : 0000000000000000 x4 : 0000000000000000 [5889.366271] x3 : 0000000000000000 x2 : 0000000000000000 [5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		

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+0x324/0x410 [hns3] [5889.394055] hns3_handle_rx_bd+0x60/0x150 [hns3] [5889.399624] hns3_clean_rx_ring+0x84/0x170 [hns3] [5889.405270] hns3_nic_common_poll+0xa8/0x220 [hns3] [5889.411084] napi_poll+0xcc/0x264 [5889.415329] net_rx_action+0xd4/0x21c [5889.419911] __do_softirq+0x130/0x358 [5889.424484] irq_exit+0x134/0x154 [5889.428700] __handle_domain_irq+0x88/0xf0 [5889.433684] gic_handle_irq+0x78/0x2c0 [5889.438319] el1_irq+0xb8/0x140 [5889.442354] arch_cpu_idle+0x18/0x40		

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+0x30/0xfc [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 Version(s): From (including) 5.15 Up to (excluding) 5.15.71					
N/A	28-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gem: Really move i915_gem_context.link under ref protection	https://git.kernel.org/stable/c/713fa3e4591f65f804bdc88e8648e219fabc9ee1, https://git.kernel.org/stable/c/d119888b09bd567e07c6b93a07f17	O-LIN-LINU-030524/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			i915_perf assumes that it can use the i915_gem_context reference to protect its i915->gem.contexts.list iteration. However, this requires 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_ioctl [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	5df88857e02, https://git.kernel.org/stable/c/f799e0568d6c153368b177e0bbbde7dcc4ce7f1d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tainted: G E 5.17.9 #180 [4070.574903] Hardware name: Intel Corporation NUC7i5BNK/NUC7i5BNB, BIOS BNKBL357.86A.0052.2017.0918.1346 09/18/2017 [4070.574907] RIP: 0010:oa_configure_all_contexts.isra.0+0x222/0x350 [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: 0000000000000002 RCX: 0000000000000000 [4070.575000] RDX: 0000000000000001 RSI: ffffc90002077b20 RDI: ffff88810ddc7c68 [4070.575004] RBP: 0000000000000001 R08: ffff888103242648 R09: fffffffffffffffc		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4070.575008] R10: ffffffff82c50bc0 R11: 0000000000025c80 R12: ffff888101bf1860 [4070.575012] R13: dead0000000000b0 R14: ffffc90002077c04 R15: ffff88810be5cabc [4070.575016] FS: 00007f1ed50c0780(0000) GS:ffff88885ec80000(0000) knlGS:0000000000000000 [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> [4070.575037] lrc_configure_all_contexts+0x13e/0x150 [i915] [4070.575103] gen8_enable_metric_set+0x4d/0x90 [i915] [4070.575164] i915_perf_open_ioctl+0xbc0/0x1500 [i915]		

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+0x1d3/0x370 [4070.575307] ? i915_oa_init_reg_state+0x110/0x110 [i915] [4070.575382] ? gen8_gt_irq_handler+0x46/0x130 [i915] [4070.575445] __x64_sys_ioctl+0x3c4/0x8d0 [4070.575451] ? __do_softirq+0xaa/0x1d2 [4070.575456] do_syscall_64+0x35/0x80 [4070.575461] entry_SYSCALL_64_after_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		

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:00007ffd65c8d7a8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [4070.575484] RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f1ed5c10397 [4070.575488] RDX: 00007ffd65c8d7c0 RSI: 0000000040106476 RDI: 0000000000000006 [4070.575492] RBP: 00005620972f9c60 R08: 000000000000000a R09: 0000000000000005 [4070.575496] R10: 000000000000000d R11: 0000000000000246 R12: 000000000000000a [4070.575500] R13: 000000000000000d R14: 0000000000000000 R15: 00007ffd65c8d7c0 [4070.575505] </TASK> [4070.575507] Modules linked in:		

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	In the Linux kernel, the following vulnerability has been resolved: gpio: mockup: Fix potential resource leakage when register a chip If creation of software node fails, the locally allocated string array is left unfreed. Free it on error path.	https://git.kernel.org/stable/c/02743c4091ccfb246f5cdbbe3f44b152d5d12933, https://git.kernel.org/stable/c/41f857033c44442a27f591fda8d986e7c9e42872, https://git.kernel.org/stable/c/9b26723e058faaf11b5	O-LIN-LINU-030524/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-48661	32fb4aa16d6849d581790	
Affected Version(s): From (including) 5.16 Up to (excluding) 5.19.12					
N/A	28-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gem: Really move i915_gem_context.link under ref protection i915_perf assumes that it can use the i915_gem_context reference to protect its i915->gem.contexts.list iteration. However, this requires 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_ioctl [i915]] filtering on	https://git.kernel.org/stable/c/713fa3e4591f65f804bdc88e8648e219fabc9ee1, https://git.kernel.org/stable/c/d119888b09bd567e07c6b93a07f175df88857e02, https://git.kernel.org/stable/c/f799e0568d6c153368b177e0bbbde7dcc4ce7f1d	O-LIN-LINU-030524/898

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/NUC7i5BNB, BIOS BNKBL357.86A.0052.2017.0918.1346 09/18/2017 [4070.574907] RIP: 0010:oa_configure_all_contexts.isra.0+0x222/0x350 [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:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000002 RCX: 0000000000000000 [4070.575000] RDX: 0000000000000001 RSI: ffffc90002077b20 RDI: ffff88810ddc7c68 [4070.575004] RBP: 0000000000000001 R08: ffff888103242648 R09: fffffffffffffc [4070.575008] R10: ffffffff82c50bc0 R11: 0000000000025c80 R12: ffff888101bf1860 [4070.575012] R13: dead0000000000b0 R14: ffffc90002077c04 R15: ffff88810be5cabc [4070.575016] FS: 00007f1ed50c0780(0000) GS:ffff88885ec80000(0000) knlGS:0000000000000000 [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>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4070.575037] lrc_configure_all_contexts+0x13e/0x150 [i915] [4070.575103] gen8_enable_metric_set+0x4d/0x90 [i915] [4070.575164] i915_perf_open_ioctl+0xbc0/0x1500 [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+0x1d3/0x370 [4070.575307] ? i915_oa_init_reg_state+0x110/0x110 [i915] [4070.575382] ? gen8_gt_irq_handler+0x46/0x130 [i915] [4070.575445] __x64_sys_ioctl+0x3c4/0x8d0 [4070.575451] ? __do_softirq+0xaa/0x1d2 [4070.575456] do_syscall_64+0x35/0x80		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4070.575461] entry_SYSCALL_64_after_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:00007ffd65c8d7a8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [4070.575484] RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f1ed5c10397 [4070.575488] RDX: 00007ffd65c8d7c0 RSI: 0000000040106476 RDI: 0000000000000006 [4070.575492] RBP: 00005620972f9c60 R08: 000000000000000a R09: 0000000000000005 [4070.575496] R10: 000000000000000d R11: 0000000000000246 R12: 000000000000000a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4070.575500] R13: 000000000000000d R14: 0000000000000000 R15: 00007ffd65c8d7c0 [4070.575505] </TASK> [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) 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.kernel.org/stable/c/016b150992eebc32c4a18f783cf2bb	O-LIN-LINU-030524/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 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:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335 kmem_cache_create+0x1c/0x28 mm/slab_common.c:390	6e2545a3d9, https://git.kernel.org/stable/c/02bcd951aa3c2cea95fb241c20802e9501940296, https://git.kernel.org/stable/c/2d6e55e0c03804e1e227b80a5746e086d6c6696c	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0x78/0xb4 fs/f2fs/xattr.c:808 f2fs_fill_super+0x1050/0x1e0c fs/f2fs/super.c:4149 mount_bdev+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__arm64_sys_mount+0x2f8/0x408 fs/namespace.c:3568 **CVE ID : CVE-2022-48659**		
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 gpiomon --num-events=3 --rising-edge gpiochip1 25 There will be a warning trace as below: Call trace: free_irq+0x204/0x360 lineevent_free+0x64/0x70 gpio_ioctl+0x598/0x6a0 __arm64_sys_ioctl+0xb4/0x100 invoke_syscall+0x5c/0x130 ..... el0t_64_sync+0x1a0/0x1a4	https://git.kernel.org/stable/c/657803b918e097e47d99d1489da83a603c36bcdd, https://git.kernel.org/stable/c/69bef19d6b9700e96285f4b4e28691cda3dcd0d1, https://git.kernel.org/stable/c/97da736cd11ae73bdf2f5e21e24446b8349e0168	O-LIN-LINU-030524/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Resource Shutdown or Release	28-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gpio: mockup: Fix potential resource leakage when register a chip If creation of software node fails, the locally allocated string array is left unfreed. Free it on error path. **CVE ID : CVE-2022-48661**	https://git.kernel.org/stable/c/02743c4091ccfb246f5cdbbe3f44b152d5d12933, https://git.kernel.org/stable/c/41f857033c44442a27f591fda8d986e7c9e42872, https://git.kernel.org/stable/c/9b26723e058faaf11b532fb4aa16d6849d581790	O-LIN-LINU-030524/901
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://git.kernel.org/stable/c/653bc5e6	O-LIN-LINU-030524/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			netfilter: ipset: fix performance regression in swap operation 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 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.	d9995d7d5f497c665b321875a626161c, https://git.kernel.org/stable/c/970709a67696b100a57b33af1a3d75fc34b747eb, https://git.kernel.org/stable/c/97f7cf1cd80eeed3b7c808b7c12463295c751001	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26910		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.80					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	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 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. 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.	https://git.kernel.org/stable/c/339ddc983bc1622341d95f244c361cda3da3a4ff, https://git.kernel.org/stable/c/3cd1d92ee1dbf3e8f988767eb75f26207397792b, https://git.kernel.org/stable/c/475426ad1ae0bfdfd8f160ed9750903799392438	O-LIN-LINU-030524/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52645		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.83					
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") 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.	https://git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a, https://git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a, https://git.kernel.org/stable/c/77fd5294ea09b21f6772ac954a121b87323cec80	O-LIN-LINU-030524/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syzbot reported: BUG: KMSAN: uninit-value in __INET_ECN_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__ipgre_rcv+0x9bc/0xbc0 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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_core net/core/dev.c:5534 [inline] __netif_receive_skb+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_internal 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+0x53b9/0x66e0 drivers/net/tun.c:2009 tun_chr_write_iter+0x3af/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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 fs/read_write.c:643		

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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b **CVE ID : CVE-2024-26882**		
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.	https://git.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/1564100 7df0f0d35fa28742b25c2a7db9dcd6895, https://git.kernel.org/stable/c/21e5fa4688e1a4d3db6b72216231b24232f75c1d	O-LIN-LINU-030524/905

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. **CVE ID : CVE-2024-26883**		
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.kernel.org/stable/c/33ec04cadb77605b71d9298311919303d390c4d5, https://git.kernel.org/stable/c/3b08cfc65f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	O-LIN-LINU-030524/906

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**		
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	https://git.kernel.org/stable/c/22079b3a423382335f47d9ed32114e6c9fe88d7c, https://git.kernel.org/stable/c/225da02acdc97af01b6bc6ce1a3e5362bf01d3fb, https://git.kernel.org/stable/c/250051acc21f9d4c5c595e4fcb55986ea08c4691	O-LIN-LINU-030524/907

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.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c2	O-LIN-LINU-030524/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aoe: fix the potential use-after-free problem 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 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	0aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc848c0a814cefc487bf755fa	

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**		
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while accessing Eth segment ------------[cut here]------------ 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	https://git.kernel.org/stable/c/185fa07000e0a81d54cf8c05414cebff14469a5c, https://git.kernel.org/stable/c/4d5e86a56615cc387d21c629f9af8fb0e958d350, https://git.kernel.org/stable/c/60ba938a8bc8c90e724c75f98e932f9fb7ae1b9d	O-LIN-LINU-030524/909

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/drivers/infiniband/hw/mlx5/wr.c:131 mlx5_ib_post_send+0x191b/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		

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_send+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		

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: 0000000000000000 RBX: 0000000000000001 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffb5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80 FS: 00007fc03b444c80(0000) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CR2: 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? show_regs+0x72/0x90 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0 ? handle_bug+0x46/0x90 ? exc_invalid_op+0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_send_nodrain+0xb/0x20 [mlx5_ib] ipoib_send+0x2ec/0x770 [ib_ipoib] ipoib_start_xmit+0x5a0/0x770 [ib_ipoib] dev_hard_start_xmit+0x8e/0x1e0 ? validate_xmit_skb_list+0x4d/0x80 sch_direct_xmit+0x116/0x3a0 __dev_xmit_skb+0x1fd/0x580 __dev_queue_xmit+0x284/0x6b0 ? _raw_spin_unlock_irq+0xe/0x50 ? __flush_work.isra.0+0x20d/0x370 ? push_pseudo_header+0x17/0x40 [ib_ipoib] neigh_connected_output+0xcd/0x110		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_finish_output2+0x179/0x480 ? __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+0x64/0x70 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0 tcp_write_xmit+0x334/0x8d0 tcp_push_one+0x3c/0x60 tcp_sendmsg_locked+0x2e1/0xac0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80 sock_write_iter+0x93/0x100 vfs_write+0x326/0x3c0 ksys_write+0xbd/0xf0 ? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_ ---truncated--- **CVE ID : CVE-2024-26907**		
NULL Pointer Dereference	17-Apr-2024	5.5	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	https://git.kernel.org/stable/c/0fbcf2366ba9888cf02eda23e35fde7f7fcc07c3, https://git.kernel.org/stable/c/11b998360d96f6c76f04a95f54b49f24d3c858e4, https://git.kernel.org/stable/c/23ec1cec	O-LIN-LINU-030524/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 0000000000000018 [5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [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	24293f9799c725941677d4e167997265	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5889.302738] x23: ffff204144f53c00 x22: 0000000000000000 [5889.309134] x21: 0000000000000000 x20: ffff204004220080 [5889.315520] x19: ffff204144f53c00 x18: 0000000000000000 [5889.321897] x17: 0000000000000000 x16: 0000000000000000 [5889.328263] x15: 0000004000140ec8 x14: 0000000000000000 [5889.334617] x13: 0000000000000000 x12: 00000000010011df [5889.340965] x11: bbfeff4d22000000 x10: 0000000000000000 [5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d [5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480 [5889.359959] x5 : 0000000000000000 x4 : 0000000000000000 [5889.366271] x3 : 0000000000000000 x2 : 0000000000000000 [5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		

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+0x324/0x410 [hns3] [5889.394055] hns3_handle_rx_bd+0x60/0x150 [hns3] [5889.399624] hns3_clean_rx_ring+0x84/0x170 [hns3] [5889.405270] hns3_nic_common_poll+0xa8/0x220 [hns3] [5889.411084] napi_poll+0xcc/0x264 [5889.415329] net_rx_action+0xd4/0x21c [5889.419911] __do_softirq+0x130/0x358 [5889.424484] irq_exit+0x134/0x154 [5889.428700] __handle_domain_irq+0x88/0xf0 [5889.433684] gic_handle_irq+0x78/0x2c0 [5889.438319] el1_irq+0xb8/0x140 [5889.442354] arch_cpu_idle+0x18/0x40		

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+0x30/0xfc [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**		
Use of Uninitialized 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	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a27342fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991737 8f7e71, https://git.ke	O-LIN-LINU-030524/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_sys_name_to_handle() and issued the following report [1]. [1] "BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 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_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94	rnel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94		

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 0000000020000240" Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to solve the problem. **CVE ID : CVE-2024-26901**		
NULL Pointer Dereference	17-Apr-2024	5.5	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.kernel.org/stable/c/2535b848fa0f42ddff3e5255cf5e742c9b77bb26, https://git.kernel.org/stable/c/369f419c097e82407dd429a202cde9a73d3ae29b, https://git.kernel.org/stable/c/3ead59bafad05f2967ae2438c0528d53244cfde5	O-LIN-LINU-030524/912

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		

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 Version(s): From (including) 5.3 Up to (excluding) 6.7.11					
Missing Release of Memory after Effective Lifetime	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md: fix kmemleak of rdev->serial	https://git.kernel.org/stable/c/4c1021ce46fc2fb6115f7e79d353941e6dcad366, https://git.kernel.org/stable/c/6cf35065	O-LIN-LINU-030524/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If kobject_add() is fail in bind_rdev_to_array(), 'rdev->serial' will be alloc not be freed, and kmemleak occurs. unreferenced object 0xffff88815a350000 (size 49152): comm "mdadm", pid 789, jiffies 4294716910 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... backtrace (crc f773277a): [<0000000058b0a453>] kmemleak_alloc+0x61/0xe0 [<00000000366adf14>] __kmalloc_large_node+0x15e/0x270 [<000000002e82961b>] __kmalloc_node.cold+0x11/0x7f [<00000000f206d60a>]	8736681b9d6b0b6e58c5c76b235bb4c4, https://git.kernel.org/stable/c/6d32c832a88513f65c2c2c9c75954ee8b387adea	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kvmalloc_node+0x74/0x150 [<0000000034bf3363>] rdev_init_serial+0x67/0x170 [<0000000010e08fe9>] mddev_create_serial_pool+0x62/0x220 [<00000000c3837bf0>] bind_rdev_to_array+0x2af/0x630 [<0000000073c28560>] md_add_new_disk+0x400/0x9f0 [<00000000770e30ff>] md_ioctl+0x15bf/0x1c10 [<000000006cfab718>] blkdev_ioctl+0x191/0x3f0 [<0000000085086a11>] vfs_ioctl+0x22/0x60 [<0000000018b656fe>] __x64_sys_ioctl+0xba/0xe0 [<00000000e54e675e>] do_syscall_64+0x71/0x150		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<000000008b0ad622>] entry_SYSCALL_64_after_hwframe+0x6c/0x74 **CVE ID : CVE-2024-26900**		
Affected Version(s): From (including) 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 ends up doing a left-shift of 32 bits on an	https://git.kernel.org/stable/c/22079b3a423382335f47d9ed32114e6c9fe88d7c, https://git.kernel.org/stable/c/225da02acdc97af01b6bc6ce1a3e5362bf01d3fb, https://git.kernel.org/stable/c/250051acc21f9d4c5c595e4fcb55986ea08c4691	O-LIN-LINU-030524/914

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 Version(s): From (including) 5.5 Up to (excluding) 5.10.146					
N/A	28-Apr-2024	5.5	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	https://git.kernel.org/stable/c/016b150992eebc32c4a18f783cf2bb6e2545a3d9, https://git.kernel.org/stable/c/02bcd951aa3c2cea95fb241c20802e9501940296, https://git.kernel.org/stable/c/2d6e55e0c03804e1e2	O-LIN-LINU-030524/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggering panic via BUG_ON(); 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:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335 kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0x78/0xb4 fs/f2fs/xattr.c:808 f2fs_fill_super+0x1050/	27b80a5746e086d6c6696c	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x1e0c fs/f2fs/super.c:4149 mount_bdev+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 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+0x2f8/0x408 fs/namespace.c:3568 **CVE ID : CVE-2022-48659**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.210					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix performance regression in swap operation 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 destroy functions are split into two: cancelling garbage collectors safely at	https://git.kernel.org/stable/c/653bc5e6d9995d7d5f497c665b321875a626161c, https://git.kernel.org/stable/c/970709a67696b100a57b33af1a3d75fc34b747eb, https://git.kernel.org/stable/c/97f7cf1cd80eeed3b7c808b7c12463295c751001	O-LIN-LINU-030524/916

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 Version(s): From (including) 5.5 Up to (excluding) 5.10.214					
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") 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.	https://git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a, https://git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a, https://git.kernel.org/stable/c/77fd5294ea09b21f6772ac954a121b87323cec80	O-LIN-LINU-030524/917

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_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate 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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_tunnel_rcv+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __ipgre_rcv+0x9bc/0xbc0 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]		

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+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_internal 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+0x53b9/0x66e0 drivers/net/tun.c:2009 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055 call_write_iter include/linux/fs.h:2087 [inline] new_sync_write fs/read_write.c:497 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b **CVE ID : CVE-2024-26882**		
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	https://git.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/15641007df0f0d35fa28742b25c2a7db9dcd6895, https://git.kernel.org/stable/c/21e5fa4688e1a4d3db6b72216231b24232f75c1d	O-LIN-LINU-030524/918

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**		
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	https://git.kernel.org/stable/c/33ec04cadb77605b71d9298311919303d390c4d5, https://git.kernel.org/stable/c/3b08cfc65f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	O-LIN-LINU-030524/919

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**		
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem 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	https://git.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c20aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc84	O-LIN-LINU-030524/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(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 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.	8c0a814cefc487bf755fa	

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 Uninitialized 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_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a27342fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991737 8f7e71, https://git.kernel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	O-LIN-LINU-030524/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 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_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26901		
NULL Pointer Dereference	17-Apr-2024	5.5	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 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,	https://git.kernel.org/stable/c/2535b848fa0f42ddff3e5255cf5e742c9b77bb26, https://git.kernel.org/stable/c/369f419c097e82407dd429a202cde9a73d3ae29b, https://git.kernel.org/stable/c/3ead59bafad05f2967ae2438c0528d53244cfde5	O-LIN-LINU-030524/922

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);`,		

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 Version(s): From (including) 5.5 Up to (excluding) 6.1.83					
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.kernel.org/stable/c/2daa2a8e895e6dc2395f8628c011bcf1e019040d, https://git.kernel.org/stable/c/7e9422d35d574b646269ca46010a835ca074b310, https://git.kernel.org/stable/c/ab1be3f1aa7799f99155488c28eacaef65eb68fb	O-LIN-LINU-030524/923

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+0xe4/0x2f8 [btrfs] [653.315606] btrfs_alloc_tree_block+0xdc/0x998 [btrfs] [653.316421] btrfs_force_cow_block+0x220/0xe38 [btrfs] [653.317242] btrfs_cow_block+0x1ac/0x568 [btrfs] [653.318060] btrfs_search_slot+0xda2/0x19b8 [btrfs] [653.318879] btrfs_del_csums+0x1dc/0x798 [btrfs] [653.319702] __btrfs_free_extent.isra.0+0xc24/0x2028 [btrfs] [653.320538] __btrfs_run_delayed_refs+0xd3c/0x2390 [btrfs] [653.321340] btrfs_run_delayed_refs+0xae/0x290 [btrfs] [653.322140] flush_space+0x5e4/0x718 [btrfs]		

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+0x3b6/0x838 [653.323800] worker_thread+0x75e/0xb10 [653.323817] kthread+0x21a/0x230 [653.323836] __ret_from_fork+0x6c/0xb8 [653.323855] ret_from_fork+0xa/0x30 [653.323887] write to 0x000000017f5871b8 of 8 bytes by task 576 on cpu 3: [653.323906] btrfs_update_delayed_refs_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+0x50/0x70 [btrfs]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.327849] walk_up_proc+0x236/0xa50 [btrfs] [653.328633] walk_up_tree+0x21c/0x448 [btrfs] [653.329418] btrfs_drop_snapshot+0x802/0x1328 [btrfs] [653.330205] btrfs_clean_one_deleted_snapshot+0x184/0x238 [btrfs] [653.330995] cleaner_kthread+0x2b0/0x2f0 [btrfs] [653.331781] kthread+0x21a/0x230 [653.331800] __ret_from_fork+0x6c/0xb8 [653.331818] ret_from_fork+0xa/0x30 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 Version(s): From (including) 5.9 Up to (excluding) 5.10.146					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
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 gpiomon --num-events=3 --rising-edge gpiochip1 25 There will be a warning trace as below: Call trace: free_irq+0x204/0x360 lineevent_free+0x64/0x70 gpio_ioctl+0x598/0x6a0 __arm64_sys_ioctl+0xb4/0x100 invoke_syscall+0x5c/0x130 ..... el0t_64_sync+0x1a0/0x1a4 The reason of this issue is that calling request_threaded_irq() function failed, and then lineevent_free() is invoked to release	https://git.kernel.org/stable/c/657803b918e097e47d99d1489da83a603c36bcdd, https://git.kernel.org/stable/c/69bef19d6b9700e96285f4b4e28691cda3dcd0d1, https://git.kernel.org/stable/c/97da736cd11ae73bdf2f5e21e24446b8349e0168	O-LIN-LINU-030524/924

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 Version(s): From (including) 6.2 Up to (excluding) 6.6.18					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	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 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.	https://git.kernel.org/stable/c/339ddc983bc1622341d95f244c361cda3da3a4ff, https://git.kernel.org/stable/c/3cd1d92ee1dbf3e8f988767eb75f26207397792b, https://git.kernel.org/stable/c/475426ad1ae0bfdfd8f160ed9750903799392438	O-LIN-LINU-030524/925

Weakness	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**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix performance regression in swap operation 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.	https://git.kernel.org/stable/c/653bc5e6d9995d7d5f497c665b321875a626161c, https://git.kernel.org/stable/c/970709a67696b100a57b33af1a3d75fc34b747eb, https://git.kernel.org/stable/c/97f7cf1cd80eeed3b7c808b7c12463295c751001	O-LIN-LINU-030524/926

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 Version(s): From (including) 6.2 Up to (excluding) 6.6.23					
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") 1ca1ba465e55 ("geneve: make sure to	https://git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a, https://git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a, https://git.kernel.org/stable/c/77fd5294ea09b21f6772ac954a121b87323cec80	O-LIN-LINU-030524/927

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_decapsulate 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+0xed9/0x2ed0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __ipgre_rcv+0x9bc/0xbc0 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		

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+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_internal 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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tun_get_user+0x53b9/0x66e0 drivers/net/tun.c:2009 tun_chr_write_iter+0x3af/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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055 call_write_iter include/linux/fs.h:2087 [inline] new_sync_write fs/read_write.c:497 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b **CVE ID : CVE-2024-26882**		
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	https://git.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/15641007df0f0d35fa28742b25c2a7db9dcd6895,	O-LIN-LINU-030524/928

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 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.	https://git.kernel.org/stable/c/21e5fa4688e1a4d3db6b72216231b24232f75c1d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26883		
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 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.kernel.org/stable/c/33ec04cadb77605b71d9298311919303d390c4d5, https://git.kernel.org/stable/c/3b08cfc65f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	O-LIN-LINU-030524/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26884		
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 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	https://git.kernel.org/stable/c/22079b3a423382335f47d9ed32114e6c9fe88d7c, https://git.kernel.org/stable/c/225da02acdc97af01b6bc6ce1a3e5362bf01d3fb, https://git.kernel.org/stable/c/250051acc21f9d4c5c595e4fcb55986ea08c4691	O-LIN-LINU-030524/930

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**		
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem 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	https://git.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c20aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc848c0a814cefc487bf755fa	O-LIN-LINU-030524/931

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		

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**		
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while accessing Eth segment ----------[cut here]---------- memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 (size 2) WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 mlx5_ib_post_send+0x191b/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)	https://git.kernel.org/stable/c/185fa07000e0a81d54cf8c05414cebff14469a5c, https://git.kernel.org/stable/c/4d5e86a56615cc387d21c629f9af8fb0e958d350, https://git.kernel.org/stable/c/60ba938a8bc8c90e724c75f98e932f9fb7ae1b9d	O-LIN-LINU-030524/932

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		

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_send+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: 0000000000000000 RBX: 0000000000000001 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffb5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80 FS: 00007fc03b444c80(0000) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<TASK> ? show_regs+0x72/0x90 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0 ? handle_bug+0x46/0x90 ? exc_invalid_op+0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_send_nodrain+0xb/0x20 [mlx5_ib] ipoib_send+0x2ec/0x770 [ib_ipoib] ipoib_start_xmit+0x5a0/0x770 [ib_ipoib] dev_hard_start_xmit+0x8e/0x1e0		

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+0x284/0x6b0 ? _raw_spin_unlock_irq+0xe/0x50 ? __flush_work.isra.0+0x20d/0x370 ? push_pseudo_header+0x17/0x40 [ib_ipoib] neigh_connected_output+0xcd/0x110 ip_finish_output2+0x179/0x480 ? __smp_call_single_queue+0x61/0xa0 __ip_finish_output+0xc3/0x190 ip_finish_output+0x2e/0xf0 ip_output+0x78/0x110		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_ip_finish_output+0x10/0x10 ip_local_out+0x64/0x70 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0 tcp_write_xmit+0x334/0x8d0 tcp_push_one+0x3c/0x60 tcp_sendmsg_locked+0x2e1/0xac0 tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80 sock_write_iter+0x93/0x100 vfs_write+0x326/0x3c0 ksys_write+0xbd/0xf0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_ ---truncated--- **CVE ID : CVE-2024-26907**		
NULL Pointer Dereference	17-Apr-2024	5.5	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 0000000000000018	https://git.kernel.org/stable/c/0fbcf2366ba9888cf02eda23e35fde7f7fcc07c3, https://git.kernel.org/stable/c/11b998360d96f6c76f04a95f54b49f24d3c858e4, https://git.kernel.org/stable/c/23ec1cec24293f9799c725941677d4e167997265	O-LIN-LINU-030524/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [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: 0000000000000000 [5889.309134] x21: 0000000000000000 x20: ffff204004220080 [5889.315520] x19: ffff204144f53c00 x18: 0000000000000000 [5889.321897] x17: 0000000000000000 x16: 0000000000000000 [5889.328263] x15: 0000004000140ec8 x14: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5889.334617] x13: 0000000000000000 x12: 00000000010011df [5889.340965] x11: bbfeff4d22000000 x10: 0000000000000000 [5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d [5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480 [5889.359959] x5 : 0000000000000000 x4 : 0000000000000000 [5889.366271] x3 : 0000000000000000 x2 : 0000000000000000 [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+0x324/0x410 [hns3] [5889.394055] hns3_handle_rx_bd+0x60/0x150 [hns3] [5889.399624] hns3_clean_rx_ring+0x84/0x170 [hns3] [5889.405270] hns3_nic_common_poll+0xa8/0x220 [hns3]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5889.411084] napi_poll+0xcc/0x264 [5889.415329] net_rx_action+0xd4/0x21c [5889.419911] __do_softirq+0x130/0x358 [5889.424484] irq_exit+0x134/0x154 [5889.428700] __handle_domain_irq+0x88/0xf0 [5889.433684] gic_handle_irq+0x78/0x2c0 [5889.438319] el1_irq+0xb8/0x140 [5889.442354] arch_cpu_idle+0x18/0x40 [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+0x30/0xfc [5889.465523] secondary_start_kernel+0x158/0x1ec [5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80)		

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**		
Use of Uninitialized 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_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a27342fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991737 8f7e71, https://git.kernel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	O-LIN-LINU-030524/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 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_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_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.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26901		
NULL Pointer Dereference	17-Apr-2024	5.5	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 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,	https://git.kernel.org/stable/c/2535b848fa0f42ddff3e5255cf5e742c9b77bb26, https://git.kernel.org/stable/c/369f419c097e82407dd429a202cde9a73d3ae29b, https://git.kernel.org/stable/c/3ead59bafad05f2967ae2438c0528d53244cfde5	O-LIN-LINU-030524/935

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);`,		

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_refs_rsv [btrfs] /	https://git.kernel.org/stable/c/2daa2a8e895e6dc2395f8628c011bcf1e019040d, https://git.kernel.org/stable/c/7e9422d35d574b646269ca46010a835ca074b310, https://git.kernel.org/stable/c/ab1be3f1aa7799f99155488c28eacaef65eb68fb	O-LIN-LINU-030524/936

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+0xe4/0x2f8 [btrfs] [653.315606] btrfs_alloc_tree_block+0xdc/0x998 [btrfs] [653.316421] btrfs_force_cow_block+0x220/0xe38 [btrfs] [653.317242] btrfs_cow_block+0x1ac/0x568 [btrfs] [653.318060] btrfs_search_slot+0xda2/0x19b8 [btrfs] [653.318879] btrfs_del_csums+0x1dc/0x798 [btrfs] [653.319702] __btrfs_free_extent.isra.0+0xc24/0x2028 [btrfs] [653.320538] __btrfs_run_delayed_refs+0xd3c/0x2390 [btrfs] [653.321340] btrfs_run_delayed_refs+0xae/0x290 [btrfs] [653.322140] flush_space+0x5e4/0x718 [btrfs] [653.322958] btrfs_preempt_reclaim_		

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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.327849] walk_up_proc+0x236/0xa50 [btrfs] [653.328633] walk_up_tree+0x21c/0x448 [btrfs] [653.329418] btrfs_drop_snapshot+0x802/0x1328 [btrfs] [653.330205] btrfs_clean_one_deleted_snapshot+0x184/0x238 [btrfs] [653.330995] cleaner_kthread+0x2b0/0x2f0 [btrfs] [653.331781] kthread+0x21a/0x230 [653.331800] __ret_from_fork+0x6c/0xb8 [653.331818] ret_from_fork+0xa/0x30 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 Version(s): From (including) 6.3 Up to (excluding) 6.6.23					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Apr-2024	5.5	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. This has manifested itself as the display 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.	https://git.kernel.org/stable/c/2bbd65c6ca567ed8dbbfc4fb945f57ce64bef342, https://git.kernel.org/stable/c/b979f2d50a099f3402418d7ff5f26c3952fb08bb, https://git.kernel.org/stable/c/ef45aa2841e15b649e5417fe3d4de395fe462781	O-LIN-LINU-030524/937

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_bridge_attach [drm]] *ERROR* failed to attach bridge /soc@0/phy@88eb000 to encoder TMDS-31: -16		

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 0000000000000000 ... Call trace: drm_bridge_attach+0x70/0x1a8 [drm] drm_aux_bridge_attach+0x24/0x38 [aux_bridge] drm_bridge_attach+0x80/0x1a8 [drm] dp_bridge_init+0xa8/0x15c [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		

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 Version(s): From (including) 6.7 Up to (excluding) 6.7.11					
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure	https://git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a, https://git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a, https://git.kernel.org/stable/c/77fd5294ea09b21f677	O-LIN-LINU-030524/938

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()") 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_decapsulate 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]	2ac954a121b87323cec80	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KMSAN: uninit-value in ip_tunnel_rcv+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __ipgre_rcv+0x9bc/0xbc0 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+		

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+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_internal net/core/dev.c:5734 [inline] netif_receive_skb+0x58/0x660 net/core/dev.c:5793 tun_rx_batched+0x3ee/		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x980 drivers/net/tun.c:1556 tun_get_user+0x53b9/0x66e0 drivers/net/tun.c:2009 tun_chr_write_iter+0x3af/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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055 call_write_iter include/linux/fs.h:2087 [inline] new_sync_write fs/read_write.c:497 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b **CVE ID : CVE-2024-26882**		
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	https://git.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/15641007df0f0d35fa28742b25c2a7db9dcd6895,	O-LIN-LINU-030524/939

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 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.	https://git.kernel.org/stable/c/21e5fa4688e1a4d3db6b72216231b24232f75c1d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26883		
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 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.kernel.org/stable/c/33ec04cadb77605b71d9298311919303d390c4d5, https://git.kernel.org/stable/c/3b08cfc65f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	O-LIN-LINU-030524/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26884		
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 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	https://git.kernel.org/stable/c/22079b3a423382335f47d9ed32114e6c9fe88d7c, https://git.kernel.org/stable/c/225da02acdc97af01b6bc6ce1a3e5362bf01d3fb, https://git.kernel.org/stable/c/250051acc21f9d4c5c595e4fcb55986ea08c4691	O-LIN-LINU-030524/941

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**		
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem 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	https://git.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c20aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc848c0a814cefc487bf755fa	O-LIN-LINU-030524/942

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		

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**		
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while accessing Eth segment ----------[cut here]---------- memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 (size 2) WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 mlx5_ib_post_send+0x191b/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)	https://git.kernel.org/stable/c/185fa07000e0a81d54cf8c05414cebff14469a5c, https://git.kernel.org/stable/c/4d5e86a56615cc387d21c629f9af8fb0e958d350, https://git.kernel.org/stable/c/60ba938a8bc8c90e724c75f98e932f9fb7ae1b9d	O-LIN-LINU-030524/943

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		

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_send+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: 0000000000000000 RBX: 0000000000000001 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffb5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80 FS: 00007fc03b444c80(0000) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<TASK> ? show_regs+0x72/0x90 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0 ? handle_bug+0x46/0x90 ? exc_invalid_op+0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_send_nodrain+0xb/0x20 [mlx5_ib] ipoib_send+0x2ec/0x770 [ib_ipoib] ipoib_start_xmit+0x5a0/0x770 [ib_ipoib] dev_hard_start_xmit+0x8e/0x1e0		

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+0x284/0x6b0 ? _raw_spin_unlock_irq+0xe/0x50 ? __flush_work.isra.0+0x20d/0x370 ? push_pseudo_header+0x17/0x40 [ib_ipoib] neigh_connected_output+0xcd/0x110 ip_finish_output2+0x179/0x480 ? __smp_call_single_queue+0x61/0xa0 __ip_finish_output+0xc3/0x190 ip_finish_output+0x2e/0xf0 ip_output+0x78/0x110		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_ip_finish_output+0x10/0x10 ip_local_out+0x64/0x70 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0 tcp_write_xmit+0x334/0x8d0 tcp_push_one+0x3c/0x60 tcp_sendmsg_locked+0x2e1/0xac0 tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80 sock_write_iter+0x93/0x100 vfs_write+0x326/0x3c0 ksys_write+0xbd/0xf0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_ ---truncated--- **CVE ID : CVE-2024-26907**		
NULL Pointer Dereference	17-Apr-2024	5.5	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 0000000000000018	https://git.kernel.org/stable/c/0fbcf2366ba9888cf02eda23e35fde7f7fcc07c3, https://git.kernel.org/stable/c/11b998360d96f6c76f04a95f54b49f24d3c858e4, https://git.kernel.org/stable/c/23ec1cec24293f9799c725941677d4e167997265	O-LIN-LINU-030524/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [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: 0000000000000000 [5889.309134] x21: 0000000000000000 x20: ffff204004220080 [5889.315520] x19: ffff204144f53c00 x18: 0000000000000000 [5889.321897] x17: 0000000000000000 x16: 0000000000000000 [5889.328263] x15: 0000004000140ec8 x14: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5889.334617] x13: 0000000000000000 x12: 00000000010011df [5889.340965] x11: bbfeff4d22000000 x10: 0000000000000000 [5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d [5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480 [5889.359959] x5 : 0000000000000000 x4 : 0000000000000000 [5889.366271] x3 : 0000000000000000 x2 : 0000000000000000 [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+0x324/0x410 [hns3] [5889.394055] hns3_handle_rx_bd+0x60/0x150 [hns3] [5889.399624] hns3_clean_rx_ring+0x84/0x170 [hns3] [5889.405270] hns3_nic_common_poll+0xa8/0x220 [hns3]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5889.411084] napi_poll+0xcc/0x264 [5889.415329] net_rx_action+0xd4/0x21c [5889.419911] __do_softirq+0x130/0x358 [5889.424484] irq_exit+0x134/0x154 [5889.428700] __handle_domain_irq+0x88/0xf0 [5889.433684] gic_handle_irq+0x78/0x2c0 [5889.438319] el1_irq+0xb8/0x140 [5889.442354] arch_cpu_idle+0x18/0x40 [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+0x30/0xfc [5889.465523] secondary_start_kernel+0x158/0x1ec [5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80)		

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**		
Improper Locking	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: fix deadlock between bd_link_disk_holder and partition scan 'open_mutex' of gendisk is used to protect open/close block devices. But 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/modification and may suspend submitting io. At this	https://git.kernel.org/stable/c/03f12122b20b6e6028e9ed69030a49f9cffcbb75, https://git.kernel.org/stable/c/1e5c5b0abaee7b62a10b9707a62083b71ad21f62, https://git.kernel.org/stable/c/5a87c1f7993bc8ac358a3766bac5dc7126e01e98	O-LIN-LINU-030524/945

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		

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**		
Use of Uninitialized 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_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a27342fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991737 8f7e71, https://git.kernel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	O-LIN-LINU-030524/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instrument_copy_to_user include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 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_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kzalloc() instead of kmalloc() to solve the problem. **CVE ID : CVE-2024-26901**		
NULL Pointer Dereference	17-Apr-2024	5.5	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 0000000000000098 [273.320851] Oops [#1] [273.323179] Modules linked in: [273.326303] CPU: 0 PID: 1475 Comm: perf Not tainted 6.6.0-rc3+ #9	https://git.kernel.org/stable/c/34b567868777e9fd39ec5333969728a7f0cf179c, https://git.kernel.org/stable/c/3ede8e94de6b834b48b0643385e66363e7a04be9, https://git.kernel.org/stable/c/9f599ba3b9cc4bdb8ec1e3f0feddd41bf9d296d6	O-LIN-LINU-030524/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[273.332521] Hardware name: Sophgo Mango (DT) [273.336878] epc : riscv_pmu_ctr_get_width_mask+0x8/0x62 [273.342291] ra : pmu_sbi_ovf_handler+0x2e0/0x34e [273.347091] epc : ffffffff80aecd98 ra : ffffffff80aee056 sp : ffffff6e36928b0 [273.354454] gp : ffffffff821f82d0 tp : ffffffd90c353200 t0 : 0000002ade4f9978 [273.361815] t1 : 0000000000504d55 t2 : ffffffff8016cd8c s0 : ffffff6e3692a70 [273.369180] s1 : 0000000000000020 a0 : 0000000000000000 a1 : 00001a8e81800000 [273.376540] a2 : 0000003c00070198 a3 : 0000003c00db75a4 a4 : 0000000000000015 [273.383901] a5 : ffffffd7ff8804b0 a6 : 0000000000000015 a7 : 000000000000002a [273.391327] s2 : 000000000000ffff s3 : 0000000000000000 s4 : ffffffd7ff8803b0 [273.398773] s5 : 0000000000504d55 s6		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			: ffffffd905069800 s7 : ffffffff821fe210 [273.406139] s8 : 000000007fffffff s9 : ffffffd7ff8803b0 s10: ffffffd903f29098 [273.413660] s11: 0000000080000000 t3 : 0000000000000003 t4 : ffffffff8017a0ca [273.421022] t5 : ffffffff8023cfc2 t6 : ffffffd9040780e8 [273.426437] status: 0000000200000100 badaddr: 0000000000000098 cause: 000000000000000d [273.434512] [<ffffffff80aecd98>] riscv_pmu_ctr_get_width_mask+0x8/0x62 [273.441169] [<ffffffff80076bd8>] handle_percpu_devid_irq+0x98/0x1ee [273.447562] [<ffffffff80071158>] generic_handle_domain_irq+0x28/0x36 [273.454151] [<ffffffff8047a99a>] riscv_intc_irq+0x36/0x4e [273.459659] [<ffffffff80c944de>] handle_riscv_irq+0x4a/0x74		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[273.465442] [<ffffffff80c94c48>] do_irq+0x62/0x92 [273.470360] Code: 0420 60a2 6402 5529 0141 8082 0013 0000 0013 0000 (6d5c) b783 [273.477921] ---[end trace 0000000000000000]--- [273.482630] Kernel panic - not syncing: Fatal exception in interrupt **CVE ID : CVE-2024-26902**		
NULL Pointer Dereference	17-Apr-2024	5.5	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 cause of this bug as follows:	https://git.kernel.org/stable/c/2535b848fa0f42ddff3e5255cf5e742c9b77bb26, https://git.kernel.org/stable/c/369f419c097e82407dd429a202cde9a73d3ae29b, https://git.kernel.org/stable/c/3ead59bafad05f2967ae2438c0528d53244cfde5	O-LIN-LINU-030524/948

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		

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	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	https://git.kernel.org/stable/c/2daa2a8e895e6dc2395f8628c011bcf1e019040d, https://git.kernel.org/stable/c/7e9422d35d574b646269ca46010a835ca074b310, https://git.ke	O-LIN-LINU-030524/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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_refs_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+0xe4/0x2f8 [btrfs] [653.315606] btrfs_alloc_tree_block+0xdc/0x998 [btrfs] [653.316421] btrfs_force_cow_block+0x220/0xe38 [btrfs] [653.317242] btrfs_cow_block+0x1ac/0x568 [btrfs] [653.318060] btrfs_search_slot+0xda2/0x19b8 [btrfs]	rnel.org/stable/c/ab1be3f1aa7799f99155488c28eacaef65eb68fb	

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_refs+0xd3c/0x2390 [btrfs] [653.321340] btrfs_run_delayed_refs+0xae/0x290 [btrfs] [653.322140] flush_space+0x5e4/0x718 [btrfs] [653.322958] btrfs_preempt_reclaim_metadata_space+0x102/0x2f8 [btrfs] [653.323781] process_one_work+0x3b6/0x838 [653.323800] worker_thread+0x75e/0xb10 [653.323817] kthread+0x21a/0x230 [653.323836] __ret_from_fork+0x6c/0xb8 [653.323855] ret_from_fork+0xa/0x30 [653.323887] write to 0x000000017f5871b8 of 8 bytes by task 576 on cpu 3:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.323906] btrfs_update_delayed_refs_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+0x50/0x70 [btrfs] [653.327849] walk_up_proc+0x236/0xa50 [btrfs] [653.328633] walk_up_tree+0x21c/0x448 [btrfs] [653.329418] btrfs_drop_snapshot+0x802/0x1328 [btrfs] [653.330205] btrfs_clean_one_deleted_snapshot+0x184/0x238 [btrfs] [653.330995] cleaner_kthread+0x2b0/0x2f0 [btrfs] [653.331781] kthread+0x21a/0x230 [653.331800] __ret_from_fork+0x6c/0xb8		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[653.331818] ret_from_fork+0xa/0x30 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**		
Use After Free	17-Apr-2024	5.5	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. This has manifested itself as the display	https://git.kernel.org/stable/c/2bbd65c6ca567ed8dbbfc4fb945f57ce64bef342, https://git.kernel.org/stable/c/b979f2d50a099f3402418d7ff5f26c3952fb08bb, https://git.kernel.org/stable/c/ef45aa2841e15b649e5417fe3d4de395fe462781	O-LIN-LINU-030524/950

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:		

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_bridge_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 0000000000000000 ... Call trace: drm_bridge_attach+0x70/0x1a8 [drm] drm_aux_bridge_attach+0x24/0x38 [aux_bridge] drm_bridge_attach+0x80/0x1a8 [drm] dp_bridge_init+0xa8/0x15c [msm]		

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']		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-26909		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.7.6					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	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 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. 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.	https://git.kernel.org/stable/c/339ddc983bc1622341d95f244c361cda3da3a4ff, https://git.kernel.org/stable/c/3cd1d92ee1dbf3e8f988767eb75f26207397792b, https://git.kernel.org/stable/c/475426ad1ae0bfdfd8f160ed9750903799392438	O-LIN-LINU-030524/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52645		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Apr-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix performance regression in swap operation 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 destroy functions are split into two: cancelling garbage collectors safely at	https://git.kernel.org/stable/c/653bc5e6d9995d7d5f497c665b321875a626161c, https://git.kernel.org/stable/c/970709a67696b100a57b33af1a3d75fc34b747eb, https://git.kernel.org/stable/c/97f7cf1cd80eeed3b7c808b7c12463295c751001	O-LIN-LINU-030524/952

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 Version(s): From (including) 6.8 Up to (excluding) 6.8.2					
N/A	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") 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.	https://git.kernel.org/stable/c/5c03387021cfa3336b97e0dcba38029917a8af2a, https://git.kernel.org/stable/c/60044ab84836359534bd7153b92e9c1584140e4a, https://git.kernel.org/stable/c/77fd5294ea09b21f6772ac954a121b87323cec80	O-LIN-LINU-030524/953

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_decapsulate 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+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate 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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_tunnel_rcv+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __ipgre_rcv+0x9bc/0xbc0 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]		

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+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_internal 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+0x53b9/0x66e0 drivers/net/tun.c:2009 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055 call_write_iter include/linux/fs.h:2087 [inline] new_sync_write fs/read_write.c:497 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_write+0xb6b/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/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/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b **CVE ID : CVE-2024-26882**		
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	https://git.kernel.org/stable/c/0971126c8164abe2004b8536b49690a0d6005b0a, https://git.kernel.org/stable/c/15641007df0f0d35fa28742b25c2a7db9dcd6895, https://git.kernel.org/stable/c/21e5fa4688e1a4d3db6b72216231b24232f75c1d	O-LIN-LINU-030524/954

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**		
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	https://git.kernel.org/stable/c/33ec04cadb77605b71d9298311919303d390c4d5, https://git.kernel.org/stable/c/3b08cfc65f07b1132c1979d73f014ae6e04de55d, https://git.kernel.org/stable/c/64f00b4df0597590b199b62a37a165473bf658a6	O-LIN-LINU-030524/955

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**		
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	https://git.kernel.org/stable/c/22079b3a423382335f47d9ed32114e6c9fe88d7c, https://git.kernel.org/stable/c/225da02acdc97af01b6bc6ce1a3e5362bf01d3fb, https://git.kernel.org/stable/c/250051acc21f9d4c5c59	O-LIN-LINU-030524/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 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**	5e4fcb55986ea08c4691	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem 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 potential code execution. In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial	https://git.kernel.org/stable/c/079cba4f4e307c69878226fdf5228c20aa1c969c, https://git.kernel.org/stable/c/1a54aa506b3b2f31496731039e49778f54eee881, https://git.kernel.org/stable/c/74ca3ef68d2f449bc848c0a814cefc487bf755fa	O-LIN-LINU-030524/957

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**		
NULL Pointer Dereference	17-Apr-2024	5.5	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	https://git.kernel.org/stable/c/0fbcf2366ba9888cf02eda23e35fde7f7fcc07c3, https://git.kernel.org/stable/c/11b998360d96f6c76f04a95f54b49f24d3c858e4, https://git.kernel.org/stable/c/23ec1cec24293f9799c	O-LIN-LINU-030524/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 0000000000000018 [5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [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	725941677d4e167997265	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[5889.302738] x23: ffff204144f53c00 x22: 0000000000000000 [5889.309134] x21: 0000000000000000 x20: ffff204004220080 [5889.315520] x19: ffff204144f53c00 x18: 0000000000000000 [5889.321897] x17: 0000000000000000 x16: 0000000000000000 [5889.328263] x15: 0000004000140ec8 x14: 0000000000000000 [5889.334617] x13: 0000000000000000 x12: 00000000010011df [5889.340965] x11: bbfeff4d22000000 x10: 0000000000000000 [5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d [5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480 [5889.359959] x5 : 0000000000000000 x4 : 0000000000000000 [5889.366271] x3 : 0000000000000000 x2 : 0000000000000000 [5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080		

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+0x324/0x410 [hns3] [5889.394055] hns3_handle_rx_bd+0x60/0x150 [hns3] [5889.399624] hns3_clean_rx_ring+0x84/0x170 [hns3] [5889.405270] hns3_nic_common_poll+0xa8/0x220 [hns3] [5889.411084] napi_poll+0xcc/0x264 [5889.415329] net_rx_action+0xd4/0x21c [5889.419911] __do_softirq+0x130/0x358 [5889.424484] irq_exit+0x134/0x154 [5889.428700] __handle_domain_irq+0x88/0xf0 [5889.433684] gic_handle_irq+0x78/0x2c0 [5889.438319] el1_irq+0xb8/0x140 [5889.442354] arch_cpu_idle+0x18/0x40		

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+0x30/0xfc [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**		
Improper Locking	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: fix deadlock between bd_link_disk_holder and partition scan 'open_mutex' of gendisk is used to protect	https://git.kernel.org/stable/c/03f12122b20b6e6028e9ed69030a49f9cffcbb75, https://git.kernel.org/stable/c/1e5c5b0ababee7b62a10b9707a62083b71ad21f62, https://git.ke	O-LIN-LINU-030524/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			open/close block devices. But 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/modification 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 ... md_submit_bio md_ioctl mddev_syspend -> suspend all io	rnel.org/stable/c/5a87c1f7993bc8ac358a3766bac5dc7126e01e98	

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 after Effective Lifetime	17-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md: fix kmemleak of rdev->serial	https://git.kernel.org/stable/c/4c1021ce46fc2fb6115f7e79d353941e6dcad366, https://git.kernel.org/stable/c/6cf35065	O-LIN-LINU-030524/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If kobject_add() is fail in bind_rdev_to_array(), 'rdev->serial' will be alloc not be freed, and kmemleak occurs. unreferenced object 0xffff88815a350000 (size 49152): comm "mdadm", pid 789, jiffies 4294716910 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... backtrace (crc f773277a): [<0000000058b0a453>] kmemleak_alloc+0x61/0xe0 [<00000000366adf14>] __kmalloc_large_node+0x15e/0x270 [<000000002e82961b>] __kmalloc_node.cold+0x11/0x7f [<00000000f206d60a>]	8736681b9d6b0b6e58c5c76b235bb4c4, https://git.kernel.org/stable/c/6d32c832a88513f65c2c2c9c75954ee8b387adea	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kvmalloc_node+0x74/0x150 [<0000000034bf3363>] rdev_init_serial+0x67/0x170 [<0000000010e08fe9>] mddev_create_serial_pool+0x62/0x220 [<00000000c3837bf0>] bind_rdev_to_array+0x2af/0x630 [<0000000073c28560>] md_add_new_disk+0x400/0x9f0 [<00000000770e30ff>] md_ioctl+0x15bf/0x1c10 [<000000006cfab718>] blkdev_ioctl+0x191/0x3f0 [<0000000085086a11>] vfs_ioctl+0x22/0x60 [<0000000018b656fe>] __x64_sys_ioctl+0xba/0xe0 [<00000000e54e675e>] do_syscall_64+0x71/0x150		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<000000008b0ad622>] entry_SYSCALL_64_after_hwframe+0x6c/0x74 **CVE ID : CVE-2024-26900**		
Use of Uninitialized 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_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user include/linux/instrumented.h:114 [inline]	https://git.kernel.org/stable/c/3948abaa4e2be938ccdfc289385a27342fb13d43, https://git.kernel.org/stable/c/423b6bdf19bbc5e1f7e746104509991 7378f7e71, https://git.kernel.org/stable/c/4bac28f441e3cc9d3f1a84c8d023228a68d8a7c1	O-LIN-LINU-030524/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_copy_to_user+0xbc/0x100 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_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc+0x121/0x3c0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_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**		