National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

https://nciipc.gov.in

16 - 31 Jan 2021 Vol. 08 No. 02

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Hardware					
Asus					
dsl-n14u_b1					
Unrestricted Upload of File with Dangerous Type	18-Jan-21	5	An issue was discovered on ASUS DSL-N14U-B1 1.1.2.3_805 devices. An attacker can upload arbitrary file content as a firmware update when the filename Settings_DSL-N14U-B1.trx is used. Once this file is loaded, shutdown measures on a wide range of services are triggered as if it were a real update, resulting in a persistent outage of those services. **CVE ID : CVE-2021-3166**	N/A	H-ASU-DSL--010221/1
Cisco					
vedge_1000_router					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	H-CIS-VEDG-010221/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/3
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/4
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-	H-CIS-VEDG-010221/5

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	cmdinjm-9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/6
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/7
Improper Restriction of Operations within the	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-VEDG-010221/8

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	yAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/9
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/10
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/11

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/12
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/13
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/14
Buffer Copy	20-Jan-21	7.5	Multiple vulnerabilities in	https://tools	H-CIS-VEDG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	010221/15
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/16
vedge_100_router					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	H-CIS-VEDG-010221/17

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/18
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/19
Improper Neutralization of Special Elements used in a Command	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	H-CIS-VEDG-010221/20

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	sco-sa-sdwan-cmdinjm-9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/21
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/22
Improper Restriction of	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated,	https://tools.cisco.com/security/cent	H-CIS-VEDG-010221/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	er/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/24
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/25
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-	H-CIS-VEDG-010221/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advisory. **CVE ID : CVE-2021-1279**	48jJuEUP	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/27
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/28
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-	H-CIS-VEDG-010221/29

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1300	B5NrSHbj	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/30
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/31
vedge_100b_router					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	H-CIS-VEDG-010221/32

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/33
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/34
Improper Neutralization of Special Elements	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform	https://tools.cisco.com/security/center/content/	H-CIS-VEDG-010221/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/36
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/37
Improper	20-Jan-21	7.8	Multiple vulnerabilities in	https://tools	H-CIS-VEDG-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	010221/38
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/39
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/40
Improper Restriction of Operations within the Bounds of a Memory	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-VEDG-010221/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	sdwan-dosmulti-48jJuEUP	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/42
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/43
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-VEDG-010221/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2021-1300**	sdwan-bufovulns-B5NrSHbj	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/45
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/46
vedge_100m_router					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-	H-CIS-VEDG-010221/47

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**	infodis-2-UPO232DG	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/48
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/49
Improper Neutralizatio	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could	https://tools.cisco.com/s	H-CIS-VEDG-010221/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/51
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/52

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1263		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/53
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/54
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/55
Improper Restriction of Operations within the	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-VEDG-010221/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	yAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/57
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/58
Buffer Copy without Checking Size of Input ('Classic	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-VEDG-010221/59

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	yAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/60
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/61
vedge_100wm_router					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	H-CIS-VEDG-010221/62

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**	sco-sa-sdwan-infodis-2-UPO232DG	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/63
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/64

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/65
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/66
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2021-1263**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/68
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/69
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/70
Improper Restriction of Operations	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/	H-CIS-VEDG-010221/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/72
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/73
Buffer Copy without Checking Size of Input	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/	H-CIS-VEDG-010221/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/75
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/76
vedge_2000_router					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-VEDG-010221/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**	yAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/78
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/79

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1260		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/80
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/81
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/83
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/84
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/85
Improper Restriction	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could	https://tools.cisco.com/s	H-CIS-VEDG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	010221/86
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/87
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/88
Buffer Copy without	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could	https://tools.cisco.com/s	H-CIS-VEDG-010221/89

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/90
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/91
vedge_5000_router					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated,	https://tools.cisco.com/security/cent	H-CIS-VEDG-010221/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**	er/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/93
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2021-1260**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/95
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/96
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-	H-CIS-VEDG-010221/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	9QMSmgcn	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/98
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/99
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/100

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/101
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/102
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/103

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/104
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/105
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/106
vedge_cloud_router					
Improper	20-Jan-21	4.9	A vulnerability in the CLI of	https://tools	H-CIS-VEDG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	010221/107
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/108
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/109

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/110
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/111
Improper Neutralization of Special Elements used in a Command ('Command	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-VEDG-010221/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	sdwan-cmdinjm-9QMSmgcn	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/113
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/114
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1278		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	H-CIS-VEDG-010221/116
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/117
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	H-CIS-VEDG-010221/118

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1299		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/119
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	H-CIS-VEDG-010221/120
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	H-CIS-VEDG-010221/121
Dlink					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dcs-5220					
Out-of-bounds Write	19-Jan-21	7.7	** UNSUPPORTED WHEN ASSIGNED ** D-Link DCS-5220 devices have a buffer overflow. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-3182**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10203	H-DLI-DCS--010221/122
hpe					
cloudline_cl3100_gen10_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/123
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2021-25125**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/125
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/126
Improper Limitation of a Pathname to a Restricted Directory ('Path	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-CLOU-010221/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	hpesbhf04073en_us	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/129
Buffer Copy without Checking Size of Input	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?	H-HPE-CLOU-010221/130

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	docLocale=en_US&docId=emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/133
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/134
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/136
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/137
cloudline_cl4100_gen10_server					
Improper Limitation of a Pathname to a Restricted Directory	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId	H-HPE-CLOU-010221/138

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	=emr_na-hpesbhf04073en_us	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/139
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/140
Buffer Copy	29-Jan-21	7.2	The Baseboard Management	https://supp	H-HPE-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	ort.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	CLOU-010221/141
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/142
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			path traversal vulnerability. **CVE ID : CVE-2021-25129**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/144
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/145
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf0407	H-HPE-CLOU-010221/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	3en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/147
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/148
Buffer Copy without Checking Size of Input	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?	H-HPE-CLOU-010221/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	docLocale=en_US&docId=emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/150
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/152
cloudline_cl5800_gen10_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/153
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/155
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/156
Improper Limitation of a Pathname to a	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?	H-HPE-CLOU-010221/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	docLocale=en_US&docId=emr_na-hpesbhf04073en_us	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/158
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/159
Buffer Copy	29-Jan-21	7.2	The Baseboard Management	https://supp	H-HPE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	ort.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	CLOU-010221/160
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/161
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			setradiusconfig_func function. **CVE ID : CVE-2021-25133**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/163
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf0407	H-HPE-CLOU-010221/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	3en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/166
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/167
cloudline_cl5200_gen9_server					
Improper Limitation of a Pathname	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9	https://support.hpe.com/hpsc/doc/pu	H-HPE-CLOU-010221/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	blic/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/169
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25126		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/171
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/172
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/174
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/175
Buffer Copy without Checking Size of Input ('Classic	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	H-HPE-CLOU-010221/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	n_US&docId =emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId =emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/177
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId =emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/178
Buffer Copy	29-Jan-21	7.2	The Baseboard Management	https://supp	H-HPE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	ort.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	CLOU-010221/179
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			startflash_func function. **CVE ID : CVE-2021-25137**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/182
cloudline_cl5800_gen9_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/183
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf0407	H-HPE-CLOU-010221/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	3en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/185
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/186
Improper Limitation of	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE	https://support.hpe.com/	H-HPE-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	010221/187
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/188
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25130		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/190
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/191
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/193
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/194
Buffer Copy without Checking Size of Input ('Classic	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	H-HPE-CLOU-010221/195

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	n_US&docId=emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/196
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	H-HPE-CLOU-010221/197
Nvidia					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jetson_tx1					
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/a_id/5148	H-NVI-JETS-010221/198
jetson_agx_xavier					
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/a_id/5148	H-NVI-JETS-010221/199
jetson_nano					
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/a_id/5148	H-NVI-JETS-010221/200
jetson_nano_2gb					
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due	https://nvidia.custhelp.com/app/answers/detail/a_id/5147,	H-NVI-JETS-010221/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5148	
jetson_tx2					
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/a_id/5148	H-NVI-JETS-010221/202
jetson_xavier_nx					
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/a_id/5148	H-NVI-JETS-010221/203
Operating System					
Asus					
dsl-n14u_b1_firmware					
Unrestricted Upload of File with Dangerous Type	18-Jan-21	5	An issue was discovered on ASUS DSL-N14U-B1 1.1.2.3_805 devices. An attacker can upload arbitrary file content as a firmware update when the filename Settings_DSL-N14U-B1.trx is used. Once this file is loaded,	N/A	O-ASU-DSL--010221/204

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			shutdown measures on a wide range of services are triggered as if it were a real update, resulting in a persistent outage of those services. **CVE ID : CVE-2021-3166**		
Cisco					
sd-wan_vsmart_controller_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-SD-W-010221/205
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/206
Improper Neutralization of Special Elements	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform	https://tools.cisco.com/security/center/content/	O-CIS-SD-W-010221/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/208
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/209
Improper	20-Jan-21	7.8	Multiple vulnerabilities in	https://tools	O-CIS-SD-W-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	010221/210
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-SD-W-010221/211
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-SD-W-010221/212
Improper Restriction of Operations within the Bounds of a Memory	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-SD-W-010221/213

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	sdwan-dosmulti-48jJuEUP	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/214
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/215
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-SD-W-010221/216

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2021-1300**	sdwan-bufovulns-B5NrSHbj	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	O-CIS-SD-W-010221/217
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	O-CIS-SD-W-010221/218
sd-wan_firmware					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-	O-CIS-SD-W-010221/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**	infodis-2-UPO232DG	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-SD-W-010221/220
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/221
Improper Neutralizatio	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could	https://tools.cisco.com/s	O-CIS-SD-W-010221/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/223
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1263		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-SD-W-010221/225
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-SD-W-010221/226
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-SD-W-010221/227
Improper Restriction of Operations within the	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurit	O-CIS-SD-W-010221/228

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	yAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/229
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	O-CIS-SD-W-010221/230
Buffer Copy without Checking Size of Input ('Classic	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected	https://tools.cisco.com/security/center/content/CiscoSecurit	O-CIS-SD-W-010221/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	yAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	O-CIS-SD-W-010221/232
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	O-CIS-SD-W-010221/233
ios_xe_sd-wan					
Improper Restriction of Operations within the Bounds of a	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	O-CIS-IOS_-010221/234

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	sco-sa-sdwan-dosmulti-48jJuEUP	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-IOS_-010221/235
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-IOS_-010221/236
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-IOS_-010221/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	O-CIS-IOS_-010221/238
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	O-CIS-IOS_-010221/239
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	O-CIS-IOS_-010221/240
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-	O-CIS-IOS_-010221/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	TnGFHrS	
Debian					
debian_linux					
Uncontrolled Resource Consumption	19-Jan-21	4.3	rfc822.c in Mutt through 2.0.4 allows remote attackers to cause a denial of service (mailbox unavailability) by sending email messages with sequences of semicolon characters in RFC822 address fields (aka terminators of empty groups). A small email message from the attacker can cause large memory consumption, and the victim may then be unable to see email messages from other persons. **CVE ID : CVE-2021-3181**	https://gitlab.com/muttmua/mutt/-/commit/4a2becbdb4422aaffe3ce314991b9d670b7adf17, https://gitlab.com/muttmua/mutt/-/commit/939b02b33ae29bc0d642570c1dcfd4b339037d19, https://gitlab.com/muttmua/mutt/-/commit/d4305208955c5cdd9fe96dfa61e7c1e14e176a14	O-DEB-DEBI-010221/242
Dlink					
dcs-5220_firmware					
Out-of-bounds	19-Jan-21	7.7	** UNSUPPORTED WHEN ASSIGNED ** D-Link DCS-	https://supportannounce	O-DLI-DCS--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			5220 devices have a buffer overflow. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-3182**	ment.us.dlink.com/announcement/publication.aspx?name=SAP10203	010221/243
Fedoraproject					
fedora					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Jan-21	7.5	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely. **CVE ID : CVE-2021-3177**	https://bugs.python.org/issue42938, https://github.com/python/cpython/pull/24239, https://python-security.readthedocs.io/vuln/ctypes-buffer-overflow-pycarg_repr.html	O-FED-FEDO-010221/244
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-21	5.5	** DISPUTED ** fs/nfsd/nfs3xdr.c in the Linux kernel through 5.10.8, when there is an NFS export of a subdirectory of a filesystem, allows remote attackers to traverse to other parts of the filesystem via READDIRPLUS. NOTE: some parties argue that such a subdirectory export is not intended to prevent this attack; see also the exports(5) no_subtree_check default behavior.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=51b2ee7d006a736a9126e8111d1f24e4fd0afaa6, https://patchwork.kernel.org/project/linux-	O-FED-FEDO-010221/245

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3178	nfs/patch/20210111210129.GA11652@fieldses.org/	
Google					
android					
Not Available	20-Jan-21	4.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the implementation of the RPMB command status, in which an attacker can write to the Write Protect Configuration Block, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2021-1067**	https://nvidia.custhelp.com/app/answers/detail/a_id/5148	O-GOO-ANDR-010221/246
Out-of-bounds Read	20-Jan-21	4.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVDEC component, in which an attacker can read from or write to a memory location that is outside the intended boundary of the buffer, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2021-1068**	https://nvidia.custhelp.com/app/answers/detail/a_id/5148	O-GOO-ANDR-010221/247
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/	O-GOO-ANDR-010221/248

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				a_id/5148	
hpe					
cloudline_cl3100_gen10_server_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/249
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/250
Buffer Copy without Checking Size of Input ('Classic Buffer	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-CLOU-010221/251

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/252
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/253
Improper Limitation of	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE	https://support.hpe.com/	O-HPE-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	010221/254
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25131		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/257
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/258
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/260
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/261
Buffer Copy without Checking Size of Input ('Classic	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	O-HPE-CLOU-010221/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	n_US&docId =emr_na-hpesbhf0407 3en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId =emr_na-hpesbhf0407 3en_us	O-HPE-CLOU-010221/263
cloudline_cl4100_gen10_server_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId =emr_na-hpesbhf0407 3en_us	O-HPE-CLOU-010221/264
Improper	29-Jan-21	7.2	The Baseboard Management	https://supp	O-HPE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	ort.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	CLOU-010221/265
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/267

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/268
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/269
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-CLOU-010221/270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/271
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/272
Buffer Copy without Checking	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9	https://support.hpe.com/hpsc/doc/pu	O-HPE-CLOU-010221/273

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	blic/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/274
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25135		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/276
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/277
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/278

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**		
cloudline_cl5200_gen9_server_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/279
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/280
Buffer Copy without Checking Size of Input	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?	O-HPE-CLOU-010221/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	docLocale=en_US&docId=emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/282
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25128		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/284
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/285
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/287
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/288
Buffer Copy without Checking Size of Input ('Classic Buffer	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId	O-HPE-CLOU-010221/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	=emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/291
Buffer Copy	29-Jan-21	7.2	The Baseboard Management	https://supp	O-HPE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	ort.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	CLOU-010221/292
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/293
cloudline_cl5800_gen10_server_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/296
Buffer Copy without Checking Size of Input ('Classic Buffer	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId	O-HPE-CLOU-010221/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	=emr_na-hpesbhf04073en_us	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/298
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/299
Buffer Copy without	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE	https://support.hpe.com/	O-HPE-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	010221/300
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/301
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25132		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/303
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/304
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function. **CVE ID : CVE-2021-25136**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/306
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/307
Buffer Copy without Checking Size of Input ('Classic	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	O-HPE-CLOU-010221/308

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	n_US&docId=emr_na-hpesbhf04073en_us	
cloudline_cl5800_gen9_server_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice deletevideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25124**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/309
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice delsolrecordedvideo_func function path traversal vulnerability. **CVE ID : CVE-2021-25125**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/310

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice downloadkvmjnlp_func function. **CVE ID : CVE-2021-25126**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/311
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice generatesslcertificate_func function. **CVE ID : CVE-2021-25127**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/312
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/313

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local spx_restservice gethelpdata_func function path traversal vulnerability. **CVE ID : CVE-2021-25128**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local spx_restservice getvideodata_func function path traversal vulnerability. **CVE ID : CVE-2021-25129**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/314
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setactdir_func function. **CVE ID : CVE-2021-25130**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-CLOU-010221/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setfwimagelocation_func function. **CVE ID : CVE-2021-25131**	hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setmediaconfig_func function. **CVE ID : CVE-2021-25132**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/317
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setradiusconfig_func function. **CVE ID : CVE-2021-25133**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/318
Buffer Copy without Checking	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9	https://support.hpe.com/hpsc/doc/pu	O-HPE-CLOU-010221/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setremoteimageinfo_func function. **CVE ID : CVE-2021-25134**	blic/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsmtp_func function. **CVE ID : CVE-2021-25135**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/320
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice setsolvideoremotestorage_func function.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25136		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice startflash_func function. **CVE ID : CVE-2021-25137**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/322
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Jan-21	7.2	The Baseboard Management Controller(BMC) in HPE Cloudline CL5800 Gen9 Server; HPE Cloudline CL5200 Gen9 Server; HPE Cloudline CL4100 Gen10 Server; HPE Cloudline CL3100 Gen10 Server; HPE Cloudline CL5800 Gen10 Server BMC firmware has a local buffer overlfow in spx_restservice uploadsshkey function. **CVE ID : CVE-2021-25138**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04073en_us	O-HPE-CLOU-010221/323
Linux					
linux_kernel					
Improper Limitation of a Pathname to a Restricted Directory ('Path	19-Jan-21	5.5	** DISPUTED ** fs/nfsd/nfs3xdr.c in the Linux kernel through 5.10.8, when there is an NFS export of a subdirectory of a filesystem, allows remote attackers to traverse to other parts of the filesystem via READDIRPLUS.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=51b2ee7d006a736	O-LIN-LINU-010221/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			NOTE: some parties argue that such a subdirectory export is not intended to prevent this attack; see also the exports(5) no_subtree_check default behavior. **CVE ID : CVE-2021-3178**	a9126e8111d1f24e4fd0afaa6, https://patchwork.kernel.org/project/linux-nfs/patch/20210111210129.GA11652@fieldses.org/	
Microsoft					
windows					
Not Available	20-Jan-21	5.1	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: CVE-2021-2018 affects Windows platform only. CVSS 3.1 Base Score 8.3	https://www.oracle.com/security-alerts/cpujan2021.html	O-MIC-WIND-010221/325

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2018**		
Nvidia					
linux_for_tegra					
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/a_id/5148	O-NVI-LINU-010221/326
Oracle					
zfs_storage_appliance					
Not Available	20-Jan-21	2.1	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all	https://www.oracle.com/security-alerts/cpujan2021.html	O-ORA-ZFS_-010221/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java VM accessible data. CVSS 3.1 Base Score 4.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-1993**		
Not Available	20-Jan-21	1.2	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: RAS subsystems). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle ZFS Storage Appliance Kit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2021-1999**	https://www.oracle.com/security-alerts/cpujan2021.html	O-ORA-ZFS_-010221/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
async-git_project					
async-git					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jan-21	7.5	The async-git package before 1.13.2 for Node.js allows OS Command Injection via shell metacharacters, as demonstrated by git.reset and git.tag. **CVE ID : CVE-2021-3190**	https://github.com/omrilotan/async-git/pull/13/commits/611823bd97dd41e9e8127c38066868ff9dcfa57a, https://github.com/omrilotan/async-git/pull/13/commits/a5f45f58941006c4cc1699609383b533d9b92c6a, https://github.com/omrilotan/async-git/pull/14	A-ASY-ASYN-010221/329
bigprof					
online_invoicing_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-21	3.5	Online Invoicing System (OIS) is open source software which is a lean invoicing system for small businesses, consultants and freelancers created using AppGini. In OIS version 4.0 there is a stored XSS which can enables an attacker takeover of the admin account through a payload that extracts a csrf token and sends a request to	https://github.com/bigprof-software/online-invoicing-system/security/advisories/GHSA-rm79-5596-r7q4	A-BIG-ONLI-010221/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			change password. It has been found that Item description is reflected without sanitization in app/items_view.php which enables the malicious scenario. **CVE ID : CVE-2021-21260**		
Cisco					
content_security_management_appliance					
Insertion of Sensitive Information Into Sent Data	20-Jan-21	5	A vulnerability in the authentication for the general purpose APIs implementation of Cisco Email Security Appliance (ESA), Cisco Content Security Management Appliance (SMA), and Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to access general system information and certain configuration information from an affected device. The vulnerability exists because a secure authentication token is not required when authenticating to the general purpose API. An attacker could exploit this vulnerability by sending a crafted request for information to the general purpose API on an affected device. A successful exploit could allow the attacker to obtain system and configuration information from the affected device, resulting in an unauthorized	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-RHp44vAC	A-CIS-CONT-010221/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-1129**		
smart_software_manager_satellite					
Improper Input Validation	20-Jan-21	10	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1138**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A	A-CIS-SMAR-010221/332
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1139**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A	A-CIS-SMAR-010221/333
Improper Input Validation	20-Jan-21	10	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A	A-CIS-SMAR-010221/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1140		
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1141**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A	A-CIS-SMAR-010221/335
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	10	Multiple vulnerabilities in the web UI of Cisco Smart Software Manager Satellite could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1142**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A	A-CIS-SMAR-010221/336
sd-wan_vbond_orchestrator					
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	A-CIS-SD-W-010221/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/338
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/339
Improper Neutralization of Special Elements used in a Command ('Command	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-SD-W-010221/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	sdwan-cmdinjm-9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/341
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/342
Improper Restriction of Operations	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/	A-CIS-SD-W-010221/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1274**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/344
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/345
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1279		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/347
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	A-CIS-SD-W-010221/349

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	A-CIS-SD-W-010221/350
Improper Input Validation	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1305**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	A-CIS-SD-W-010221/351
web_security_virtual_appliance					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-21	3.5	A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-xss-RuB5WGqL	A-CIS-WEB_-010221/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface. **CVE ID : CVE-2021-1271**		
immunet					
Uncontrolled Search Path Element	20-Jan-21	6.9	A vulnerability in the loading mechanism of specific DLLs of Cisco Advanced Malware Protection (AMP) for Endpoints for Windows and Immunet for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on the targeted system. This file will execute when the vulnerable application launches. A successful exploit could allow the attacker to execute arbitrary code on the targeted system with SYSTEM	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-5PAZ3hRV	A-CIS-IMMU-010221/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2021-1280**		
elastic_services_controller					
Uncontrolled Resource Consumption	20-Jan-21	5	A vulnerability in the system resource management of Cisco Elastic Services Controller (ESC) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) to the health monitor API on an affected device. The vulnerability is due to inadequate provisioning of kernel parameters for the maximum number of TCP connections and SYN backlog. An attacker could exploit this vulnerability by sending a flood of crafted TCP packets to an affected device. A successful exploit could allow the attacker to block TCP listening ports that are used by the health monitor API. This vulnerability only affects customers who use the health monitor API. **CVE ID : CVE-2021-1312**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esc-dos-4Gw6D527	A-CIS-ELAS-010221/354
data_center_network_manager					
Incomplete List of Disallowed Inputs	20-Jan-21	8.5	Multiple vulnerabilities in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-api-path-	A-CIS-DATA-010221/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1133**	TpTApx2p	
Incomplete List of Disallowed Inputs	20-Jan-21	4	Multiple vulnerabilities in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1135**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-api-path-TpTApx2p	A-CIS-DATA-010221/356
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	6.5	Multiple vulnerabilities in certain REST API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to execute arbitrary SQL commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1247**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-sql-inj-OAQOObP	A-CIS-DATA-010221/357
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	6.5	Multiple vulnerabilities in certain REST API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to execute arbitrary SQL commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1248**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-sql-inj-OAQOObP	A-CIS-DATA-010221/358

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1249**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-vulns-GuUJ39gh	A-CIS-DATA-010221/359
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1250**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-vulns-GuUJ39gh	A-CIS-DATA-010221/360
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-21	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-vulns-GuUJ39gh	A-CIS-DATA-010221/361

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1253**		
Incomplete List of Disallowed Inputs	20-Jan-21	5.5	Multiple vulnerabilities in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1255**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-api-path-TpTApx2p	A-CIS-DATA-010221/362
Not Available	20-Jan-21	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1269**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-authbypass-OHBPbxu	A-CIS-DATA-010221/363
Incorrect Authorization	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. For more information about	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-authbypass-	A-CIS-DATA-010221/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1270**	OHBPbxu	
Server-Side Request Forgery (SSRF)	20-Jan-21	6.8	A vulnerability in the session validation feature of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on a targeted system. This vulnerability is due to insufficient validation of parameters in a specific HTTP request by an attacker. An attacker could exploit this vulnerability by sending a crafted HTTP request to an authenticated user of the DCNM web application. A successful exploit could allow the attacker to bypass access controls and gain unauthorized access to the Device Manager application, which provides access to network devices managed by the system. **CVE ID : CVE-2021-1272**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-ssrf-F2vX6q5p	A-CIS-DATA-010221/365
Improper Certificate Validation	20-Jan-21	5.8	Multiple vulnerabilities in Cisco Data Center Network Manager (DCNM) could allow an attacker to spoof a trusted host or construct a man-in-the-middle attack to extract sensitive information or alter certain API requests. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-cert-check-	A-CIS-DATA-010221/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient certificate validation when establishing HTTPS requests with the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1276**	BdZZV9T3	
Improper Certificate Validation	20-Jan-21	5.8	Multiple vulnerabilities in Cisco Data Center Network Manager (DCNM) could allow an attacker to spoof a trusted host or construct a man-in-the-middle attack to extract sensitive information or alter certain API requests. These vulnerabilities are due to insufficient certificate validation when establishing HTTPS requests with the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1277**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-cert-check-BdZZV9T3	A-CIS-DATA-010221/367
Memory Allocation with Excessive Size Value	20-Jan-21	2.1	A vulnerability in the logging subsystem of Cisco Data Center Network Manager (DCNM) could allow an authenticated, local attacker to view sensitive information in a system log file that should be restricted. The vulnerability exists because sensitive information is not properly masked before it is written to system log files. An attacker could exploit this vulnerability by authenticating to an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-info-disc-QCSJB6YG	A-CIS-DATA-010221/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and inspecting a specific system log file. A successful exploit could allow the attacker to view sensitive information in the system log file. To exploit this vulnerability, the attacker would need to have valid user credentials. **CVE ID : CVE-2021-1283**		
Improper Input Validation	20-Jan-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow a remote attacker with network-operator privileges to conduct a cross-site scripting (XSS) attack or a reflected file download (RFD) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1286**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-vulns-GuUJ39gh	A-CIS-DATA-010221/369
sd-wan_vmanage					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	6.4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to conduct SQL injection attacks on an affected system. These vulnerabilities exist because the web-based management interface improperly validates values in SQL queries. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-sqlinjm-xV8dsjq5	A-CIS-SD-W-010221/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on or return values from the underlying database or the operating system. **CVE ID : CVE-2021-1225**		
Improper Input Validation	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information on an affected device. The vulnerability is due to insufficient input validation of requests that are sent to the iperf tool. An attacker could exploit this vulnerability by sending a crafted request to the iperf tool, which is included in Cisco SD-WAN Software. A successful exploit could allow the attacker to obtain any file from the filesystem of an affected device. **CVE ID : CVE-2021-1233**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG	A-CIS-SD-W-010221/371
Exposure of Sensitive System Information to an Unauthorized Control Sphere	20-Jan-21	4.9	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to read sensitive database files on an affected system. The vulnerability is due to insufficient user authorization. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vinfdis-	A-CIS-SD-W-010221/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by accessing the vshell of an affected system. A successful exploit could allow the attacker to read database files from the filesystem of the underlying operating system. **CVE ID : CVE-2021-1235**	MC8L58dj	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1241**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/373
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jan-21	6.8	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain write access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to write arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-pathtrav-Z5mCVsjf	A-CIS-SD-W-010221/374

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files on the affected system. **CVE ID : CVE-2021-1259**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1260**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/375
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1261**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/376
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-	A-CIS-SD-W-010221/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1262**	9QMSmgcn	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	7.2	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1263**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/378
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1273**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/379
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-	A-CIS-SD-W-010221/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advisory. **CVE ID : CVE-2021-1274**	48jJuEUP	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1278**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/381
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jan-21	7.8	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute denial of service (DoS) attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1279**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP	A-CIS-SD-W-010221/382
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1298**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/383

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Jan-21	9	Multiple vulnerabilities in Cisco SD-WAN products could allow an authenticated attacker to perform command injection attacks against an affected device, which could allow the attacker to take certain actions with root privileges on the device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1299**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	A-CIS-SD-W-010221/384
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1300**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	A-CIS-SD-W-010221/385
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-21	7.5	Multiple vulnerabilities in Cisco SD-WAN products could allow an unauthenticated, remote attacker to execute attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1301**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj	A-CIS-SD-W-010221/386
Not Available	20-Jan-21	6	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated,	https://tools.cisco.com/security/center/content/CiscoSecurit	A-CIS-SD-W-010221/387

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1302**	yAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	
Not Available	20-Jan-21	4	Multiple vulnerabilities in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system, gain access to sensitive information, and view information that they are not authorized to access. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1304**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS	A-CIS-SD-W-010221/388
Improper Neutralization of Special Elements in Data Query Logic	20-Jan-21	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct Cypher query language injection attacks on an affected system. The vulnerability is due to insufficient input validation by the web-based	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-cql-inject-72EhnUc	A-CIS-SD-W-010221/389

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface of an affected system. A successful exploit could allow the attacker to obtain sensitive information. **CVE ID : CVE-2021-1349**		
dna_center					
Cross-Site Request Forgery (CSRF)	20-Jan-21	6.8	A vulnerability in the web-based management interface of Cisco DNA Center Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to manipulate an authenticated user into executing malicious actions without their awareness or consent. The vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a web-based management user to follow a specially crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the device with the privileges of the authenticated user. These actions include modifying the device configuration, disconnecting the user's session, and executing Command Runner	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-csrf-dC83cMcV	A-CIS-DNA_-010221/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands. **CVE ID : CVE-2021-1257**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-21	9	A vulnerability in the Command Runner tool of Cisco DNA Center could allow an authenticated, remote attacker to perform a command injection attack. The vulnerability is due to insufficient input validation by the Command Runner tool. An attacker could exploit this vulnerability by providing crafted input during command execution or via a crafted command runner API call. A successful exploit could allow the attacker to execute arbitrary CLI commands on devices managed by Cisco DNA Center. **CVE ID : CVE-2021-1264**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-cmdinj-erumsWh9	A-CIS-DNA_-010221/391
Cleartext Storage of Sensitive Information	20-Jan-21	4	A vulnerability in the configuration archive functionality of Cisco DNA Center could allow any privilege-level authenticated, remote attacker to obtain the full unmasked running configuration of managed devices. The vulnerability is due to the configuration archives files being stored in clear text, which can be retrieved by various API calls. An attacker could exploit this vulnerability by authenticating to the device and executing a series of API	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnacid-OfeeRjcn	A-CIS-DNA_-010221/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			calls. A successful exploit could allow the attacker to retrieve the full unmasked running configurations of managed devices. **CVE ID : CVE-2021-1265**		
Incorrect Privilege Assignment	20-Jan-21	6.5	A vulnerability in the user management roles of Cisco DNA Center could allow an authenticated, remote attacker to execute unauthorized commands on an affected device. The vulnerability is due to improper enforcement of actions for assigned user roles. An attacker could exploit this vulnerability by authenticating as a user with an Observer role and executing commands on the affected device. A successful exploit could allow a user with the Observer role to execute commands to view diagnostic information of the devices that Cisco DNA Center manages. **CVE ID : CVE-2021-1303**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-6qjA3hVh	A-CIS-DNA_-010221/393
email_security_appliance					
Insertion of Sensitive Information Into Sent Data	20-Jan-21	5	A vulnerability in the authentication for the general purpose APIs implementation of Cisco Email Security Appliance (ESA), Cisco Content Security Management Appliance (SMA), and Cisco Web Security Appliance (WSA)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-	A-CIS-EMAI-010221/394

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to access general system information and certain configuration information from an affected device. The vulnerability exists because a secure authentication token is not required when authenticating to the general purpose API. An attacker could exploit this vulnerability by sending a crafted request for information to the general purpose API on an affected device. A successful exploit could allow the attacker to obtain system and configuration information from the affected device, resulting in an unauthorized information disclosure. **CVE ID : CVE-2021-1129**	RHp44vAC	
unified_communications_manager					
Path Traversal: '.../...//'	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-dM687ZD6	A-CIS-UNIF-010221/395

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1357**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1364**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-dM687ZD6	A-CIS-UNIF-010221/396
Path Traversal: '.../...//'	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could	https://tools.cisco.com/security/center/content/CiscoSecurit	A-CIS-UNIF-010221/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1282**	yAdvisory/cisco-sa-imp-trav-inj-dM687ZD6	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-dM687ZD6	A-CIS-UNIF-010221/398

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1355**		
unified_communications_manager_im_and_presence_service					
Path Traversal: '.../...//'	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1357**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-dM687ZD6	A-CIS-UNIF-010221/399
Improper Neutralization of Special Elements used in an SQL Command ('SQL	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-	A-CIS-UNIF-010221/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1364**	dM687ZD6	
Path Traversal: '.../...//'	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-dM687ZD6	A-CIS-UNIF-010221/401

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2021-1282**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	4	Multiple vulnerabilities in Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an attacker to conduct path traversal attacks and SQL injection attacks on an affected system. One of the SQL injection vulnerabilities that affects Unified CM IM&amp;P also affects Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) and could allow an attacker to conduct SQL injection attacks on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1355**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-dM687ZD6	A-CIS-UNIF-010221/402
advanced_malware_protection_for_endpoints					
Uncontrolled Search Path Element	20-Jan-21	6.9	A vulnerability in the loading mechanism of specific DLLs of Cisco Advanced Malware Protection (AMP) for Endpoints for Windows and Immunet for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need valid	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-5PAZ3hRV	A-CIS-ADVA-010221/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials on the Windows system. This vulnerability is due to incorrect handling of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on the targeted system. This file will execute when the vulnerable application launches. A successful exploit could allow the attacker to execute arbitrary code on the targeted system with SYSTEM privileges. **CVE ID : CVE-2021-1280**		
web_security_appliance					
Insertion of Sensitive Information Into Sent Data	20-Jan-21	5	A vulnerability in the authentication for the general purpose APIs implementation of Cisco Email Security Appliance (ESA), Cisco Content Security Management Appliance (SMA), and Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to access general system information and certain configuration information from an affected device. The vulnerability exists because a secure authentication token is not required when authenticating to the general purpose API. An attacker could exploit this vulnerability by sending a crafted request for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-RHp44vAC	A-CIS-WEB_-010221/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information to the general purpose API on an affected device. A successful exploit could allow the attacker to obtain system and configuration information from the affected device, resulting in an unauthorized information disclosure. **CVE ID : CVE-2021-1129**		
smart_software_manager_on-prem					
URL Redirection to Untrusted Site ('Open Redirect')	20-Jan-21	4.9	A vulnerability in the web management interface of Cisco Smart Software Manager satellite could allow an authenticated, remote attacker to redirect a user to an undesired web page. The vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request that could cause the web application to redirect the request to a specified malicious URL. A successful exploit could allow the attacker to redirect a user to a malicious website. **CVE ID : CVE-2021-1218**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssmor-MDCWkT2x	A-CIS-SMAR-010221/405
Use of Hard-coded Credentials	20-Jan-21	4.6	A vulnerability in Cisco Smart Software Manager Satellite could allow an authenticated, local attacker to access sensitive information on an	https://tools.cisco.com/security/center/content/CiscoSecurit	A-CIS-SMAR-010221/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected system. The vulnerability is due to insufficient protection of static credentials in the affected software. An attacker could exploit this vulnerability by gaining access to the static credential that is stored on the local device. A successful exploit could allow the attacker to view static credentials, which the attacker could use to carry out further attacks. **CVE ID : CVE-2021-1219**	yAdvisory/cisco-sa-cssm-sc-Jd42D4Tq	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	5.5	A vulnerability in the web-based management interface of Cisco Smart Software Manager Satellite could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web-based management interface improperly validates values within SQL queries. An attacker could exploit this vulnerability by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on or return values from the underlying database or the operating system. **CVE ID : CVE-2021-1222**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-sqi-h5fDvZWp	A-CIS-SMAR-010221/407
dzzoffice					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dzzoffice					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	4.3	attach/ajax.php in DzzOffice through 2.02.1 allows XSS via the editorid parameter. **CVE ID : CVE-2021-3318**	N/A	A-DZZ-DZZO-010221/408
Fasterxml					
jackson-databind					
Deserialization of Untrusted Data	19-Jan-21	8.3	A flaw was found in jackson-databind before 2.9.10.7. FasterXML mishandles the interaction between serialization gadgets and typing. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-20190**	https://github.com/FasterXML/jackson-databind/issues/2854	A-FAS-JACK-010221/409
files					
fat_client					
Insufficient Session Expiration	19-Jan-21	5	Files.com Fat Client 3.3.6 allows authentication bypass because the client continues to have access after a logout and a removal of a login profile. **CVE ID : CVE-2021-3183**	N/A	A-FIL-FAT_-010221/410
fujielectric					
v-simulator					
Out-of-bounds Write	27-Jan-21	6.8	Multiple stack-based buffer overflow issues have been identified in the way the application processes project	N/A	A-FUJ-V-SI-010221/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22637**		
Access of Uninitialized Pointer	27-Jan-21	6.8	An uninitialized pointer issue has been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22639**	N/A	A-FUJ-V-SI-010221/412
Out-of-bounds Write	27-Jan-21	6.8	A heap-based buffer overflow issue has been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22641**	N/A	A-FUJ-V-SI-010221/413
Out-of-bounds Write	27-Jan-21	6.8	Multiple out-of-bounds write issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0).	N/A	A-FUJ-V-SI-010221/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22653		
Out-of-bounds Read	27-Jan-21	6.8	Multiple out-of-bounds read issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22655**	N/A	A-FUJ-V-SI-010221/415
v-server					
Out-of-bounds Write	27-Jan-21	6.8	Multiple stack-based buffer overflow issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22637**	N/A	A-FUJ-V-SE-010221/416
Access of Uninitialized Pointer	27-Jan-21	6.8	An uninitialized pointer issue has been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22639**	N/A	A-FUJ-V-SE-010221/417
Out-of-bounds Write	27-Jan-21	6.8	A heap-based buffer overflow issue has been identified in the way the application	N/A	A-FUJ-V-SE-010221/418

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22641**		
Out-of-bounds Write	27-Jan-21	6.8	Multiple out-of-bounds write issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22653**	N/A	A-FUJ-V-SE-010221/419
Out-of-bounds Read	27-Jan-21	6.8	Multiple out-of-bounds read issues have been identified in the way the application processes project files, allowing an attacker to craft a special project file that may allow arbitrary code execution on the Tellus Lite V-Simulator and V-Server Lite (versions prior to 4.0.10.0). **CVE ID : CVE-2021-22655**	N/A	A-FUJ-V-SE-010221/420
hgiga					
oaklouds_portal					
Incorrect Permission Assignment for Critical Resource	19-Jan-21	7.5	HGiga EIP product lacks ineffective access control in certain pages that allow attackers to access database or perform privileged functions.	https://www.chtsecurity.com/news/eb024200-7cf9-4c58-a063-	A-HGI-OAKL-010221/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22850	c451dbc9daef, https://www.twcert.org.tw/tw/cp-132-4326-3d9d2-1.html	
oaklouds_openid					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-21	7.5	HGiga EIP product contains SQL Injection vulnerability. Attackers can inject SQL commands into specific URL parameter (document management page) to obtain database schema and data. **CVE ID : CVE-2021-22851**	https://www.chtsecurity.com/news/eb024200-7cf9-4c58-a063-c451dbc9daef, https://www.twcert.org.tw/tw/cp-132-4327-50e99-1.html	A-HGI-OAKL-010221/422
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-21	6.5	HGiga EIP product contains SQL Injection vulnerability. Attackers can inject SQL commands into specific URL parameter (online registration) to obtain database schema and data. **CVE ID : CVE-2021-22852**	https://www.chtsecurity.com/news/eb024200-7cf9-4c58-a063-c451dbc9daef, https://www.twcert.org.tw/tw/cp-132-4328-97765-1.html	A-HGI-OAKL-010221/423
hyweb					
hycms-j1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-21	3.5	Hyweb HyCMS-J1 backend editing function does not filter special characters. Users after log-in can inject JavaScript syntax to perform a stored XSS (Stored Cross-site scripting) attack. **CVE ID : CVE-2021-22849**	https://www.twcert.org.tw/tw/cp-132-4318-09cd3-1.html	A-HYW-HYCM-010221/424
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jan-21	6.5	Hyweb HyCMS-J1's API fail to filter POST request parameters. Remote attackers can inject SQL syntax and execute commands without privilege. **CVE ID : CVE-2021-22847**	https://www.twcert.org.tw/tw/cp-132-4316-298fc-1.html	A-HYW-HYCM-010221/425
IBM					
collaborative_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-COLL-010221/426
engineering_insights					
Improper Neutralization of Input During Web Page	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://exchange.xforce.ibmcloud.com/vulnerabilities/19496	A-IBM-ENGI-010221/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	3, https://www.ibm.com/support/pages/node/6408694	
engineering_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-ENGI-010221/428
global_configuration_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-GLOB-010221/429
rhapsody_design_manager					
Improper	27-Jan-21	3.5	IBM Jazz Foundation	https://exch	A-IBM-RHAP-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	ange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	010221/430
rhapsody_model_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-RHAP-010221/431
rational_engineering_lifecycle_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963.	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-RATI-010221/432

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20357		
rational_quality_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-RATI-010221/433
engineering_test_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-ENGI-010221/434
engineering_workflow_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/s	A-IBM-ENGI-010221/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	upport/pages/node/6408694	
engineering_requirements_management_doors_next					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-21	3.5	IBM Jazz Foundation products is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194963. **CVE ID : CVE-2021-20357**	https://exchange.xforce.ibmcloud.com/vulnerabilities/194963, https://www.ibm.com/support/pages/node/6408694	A-IBM-ENGI-010221/436
keymaker_project					
keymaker					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jan-21	4	Keymaker is a Mastodon Community Finder based Matrix Community serverlist page Server. In Keymaker before version 0.2.0, the assets endpoint did not check for the extension. The rust `join` method without checking user input might have made it abe to do a Path Traversal attack causing to read more files than allowed. This is fixed in version 0.2.0. **CVE ID : CVE-2021-21269**	https://github.com/keymaker-mx/keymaker/commit/63f3012b390ff1519a84100df9e5dff5058bb926, https://github.com/keymaker-mx/keymaker/security/advisories/GHSA-pg25-xfcf-vjvm	A-KEY-KEYM-010221/437

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Laravel					
laravel					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Jan-21	5	Laravel is a web application framework. Versions of Laravel before 6.20.11, 7.30.2 and 8.22.1 contain a query binding exploitation. This same exploit applies to the illuminate/database package which is used by Laravel. If a request is crafted where a field that is normally a non-array value is an array, and that input is not validated or cast to its expected type before being passed to the query builder, an unexpected number of query bindings can be added to the query. In some situations, this will simply lead to no results being returned by the query builder; however, it is possible certain queries could be affected in a way that causes the query to return unexpected results. **CVE ID : CVE-2021-21263**	https://blog.laravel.com/security-laravel-62011-7302-8221-released, https://github.com/laravel/framework/pull/35865, https://github.com/laravel/framework/security/advisories/GHSA-3p32-j457-pg5x	A-LAR-LARA-010221/438
Microfocus					
application_lifecycle_management					
Improper Restriction of XML External Entity Reference	19-Jan-21	5.5	XML External Entity Injection vulnerability in Micro Focus Application Lifecycle Management (Previously known as Quality Center) product. The vulnerability affects versions 12.x, 12.60 Patch 5 and earlier, 15.0.1 Patch 2 and earlier and 15.5.	N/A	A-MIC-APPL-010221/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability could be exploited to allow an XML External Entity Injection. **CVE ID : CVE-2021-22498**		
Misp					
misp					
Weak Password Recovery Mechanism for Forgotten Password	19-Jan-21	6.4	The default setting of MISP 2.4.136 did not enable the requirements (aka require_password_confirmation) to provide the previous password when changing a password. **CVE ID : CVE-2021-25323**	https://github.com/MISP/MISP/commit/afbf95a478b6e94f532ca0776c79da1b08be7eed	A-MIS-MISP-010221/440
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-21	4.3	MISP 2.4.136 has Stored XSS in the galaxy cluster view via a cluster name to app/View/GalaxyClusters/view.ctp. **CVE ID : CVE-2021-25324**	https://github.com/MISP/MISP/commit/741243f707cac7de1a3769a38e03004f037f4a3d	A-MIS-MISP-010221/441
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-21	4.3	MISP 2.4.136 has XSS via galaxy cluster element values to app/View/GalaxyElements/ajax/index.ctp. Reference types could contain javascript: URLs. **CVE ID : CVE-2021-25325**	https://github.com/MISP/MISP/commit/829c3199ba3afdecb52e0719509f3df4463be5b4	A-MIS-MISP-010221/442
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-21	4.3	MISP 2.4.136 has XSS via a crafted URL to the app/View/Elements/global_menu.ctp user homepage favourite button. **CVE ID : CVE-2021-3184**	https://github.com/MISP/MISP/commit/8283e0fbec551f45f3f181cdb2cf29cddc23df66	A-MIS-MISP-010221/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Mutt					
mutt					
Uncontrolled Resource Consumption	19-Jan-21	4.3	rfc822.c in Mutt through 2.0.4 allows remote attackers to cause a denial of service (mailbox unavailability) by sending email messages with sequences of semicolon characters in RFC822 address fields (aka terminators of empty groups). A small email message from the attacker can cause large memory consumption, and the victim may then be unable to see email messages from other persons. **CVE ID : CVE-2021-3181**	https://gitlab.com/muttmua/mutt/-/commit/4a2becbdb4422aaffe3ce314991b9d670b7adf17, https://gitlab.com/muttmua/mutt/-/commit/939b02b33ae29bc0d642570c1dcfd4b339037d19, https://gitlab.com/muttmua/mutt/-/commit/d4305208955c5cdd9fe96dfa61e7c1e14e176a14	A-MUT-MUTT-010221/444
netsia					
seba\+					
Exposure of Sensitive Information to an Unauthorized Actor	17-Jan-21	5	Netsia SEBA+ through 0.16.1 build 70-e669dcd7 allows remote attackers to discover session cookies via a direct /session/list/allActiveSession request. For example, the attacker can discover the admin's cookie if the admin account happens to be logged in when the allActiveSession request occurs, and can then	https://www.netsia.com/#netsiaseba	A-NET-SEBA-010221/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use that cookie immediately for admin access, **CVE ID : CVE-2021-3113**		
nodered					
node-red-dashboard					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Jan-21	5	Node-RED-Dashboard before 2.26.2 allows ui_base/js/..%2f directory traversal to read files. **CVE ID : CVE-2021-3223**	https://github.com/node-red/node-red-dashboard/releases/tag/2.26.2	A-NOD-NODE-010221/446
Nvidia					
shield_experience					
Not Available	20-Jan-21	4.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the implementation of the RPMB command status, in which an attacker can write to the Write Protect Configuration Block, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2021-1067**	https://nvidia.custhelp.com/app/answers/detail/a_id/5148	A-NVI-SHIE-010221/447
Out-of-bounds Read	20-Jan-21	4.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVDEC component, in which an attacker can read from or write to a memory location that is outside the intended boundary of the buffer, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2021-1068**	https://nvidia.custhelp.com/app/answers/detail/a_id/5148	A-NVI-SHIE-010221/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Jan-21	3.6	NVIDIA SHIELD TV, all versions prior to 8.2.2, contains a vulnerability in the NVHost function, which may lead to abnormal reboot due to a null pointer reference, causing data loss. **CVE ID : CVE-2021-1069**	https://nvidia.custhelp.com/app/answers/detail/a_id/5147, https://nvidia.custhelp.com/app/answers/detail/a_id/5148	A-NVI-SHIE-010221/449
O-dyn					
collabtive					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-21	3.5	Collabtive 3.1 allows XSS when an authenticated user enters an XSS payload into the address section of the profile edit page, aka the manageuser.php?action=edit address1 parameter. **CVE ID : CVE-2021-3298**	https://collabtive.o-dyn.de/forum/viewforum.php?f=6	A-O-D-COLL-010221/450
opencats					
opencats					
Deserialization of Untrusted Data	18-Jan-21	10	OpenCATS through 0.9.5-3 unsafely deserializes index.php?m=activity requests, leading to remote code execution. This occurs because lib/DataGrid.php calls unserialize for the parametersactivity:ActivityDataGrid parameter. The PHP object injection exploit chain can leverage an __destruct magic method in guzzlehttp. **CVE ID : CVE-2021-25294**	https://github.com/snoopysecurity/snoopysecurity.github.io/blob/master/web-application-security/2021/01/16/09_opencats_php_object_injection.html, https://www.opencats.org/news/	A-OPE-OPEN-010221/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-21	4.3	OpenCATS through 0.9.5-3 has multiple Cross-site Scripting (XSS) issues. **CVE ID : CVE-2021-25295**	https://www.opencats.org/news/	A-OPE-OPEN-010221/452
opendesign					
drawings_software_development_kit					
Allocation of Resources Without Limits or Throttling	18-Jan-21	6.8	An issue was discovered in Open Design Alliance Drawings SDK before 2021.12. A memory allocation with excessive size vulnerability exists when reading malformed DGN files, which allows attackers to cause a crash, potentially enabling denial of service (crash, exit, or restart). **CVE ID : CVE-2021-25173**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-010221/453
Uncontrolled Resource Consumption	18-Jan-21	4.3	An issue was discovered in Open Design Alliance Drawings SDK before 2021.12. A memory corruption vulnerability exists when reading malformed DGN files. It can allow attackers to cause a crash, potentially enabling denial of service (Crash, Exit, or Restart). **CVE ID : CVE-2021-25174**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-010221/454
Incorrect Type Conversion or Cast	18-Jan-21	4.3	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A Type Conversion issue exists when rendering	https://www.opendesign.com/security-	A-OPE-DRAW-010221/455

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). **CVE ID : CVE-2021-25175**	advisories	
NULL Pointer Dereference	18-Jan-21	4.3	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A NULL pointer dereference exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). **CVE ID : CVE-2021-25176**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-010221/456
Incorrect Type Conversion or Cast	18-Jan-21	4.3	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A Type Confusion issue exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). **CVE ID : CVE-2021-25177**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-010221/457
Out-of-bounds Write	18-Jan-21	6.8	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A stack-based buffer overflow vulnerability exists when the recover operation is run with malformed .DXF and .DWG files. This can allow	https://www.opendesign.com/security-advisories	A-OPE-DRAW-010221/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a crash potentially enabling a denial of service attack (Crash, Exit, or Restart) or possible code execution. **CVE ID : CVE-2021-25178**		
Opmantek					
open-audit					
Insufficiently Protected Credentials	20-Jan-21	4.3	Within the Open-AudIT up to version 3.5.3 application, the web interface hides SSH secrets, Windows passwords, and SNMP strings from users using HTML 'password field' obfuscation. By using Developer tools or similar, it is possible to change the obfuscation so that the credentials are visible. **CVE ID : CVE-2021-3130**	https://opmantek.com/network-discovery-inventory-software/	A-OPM-OPEN-010221/459
Oracle					
scripting					
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks of this vulnerability can result in takeover of Oracle Scripting. CVSS 3.1 Base Score 9.8 (Confidentiality,	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-SCRI-010221/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2029**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Scripting accessible data as well as unauthorized update, insert or delete access to some of Oracle Scripting accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2091**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-SCRI-010221/461
common_applications_calendar					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Tasks). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2034**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-COMM-010221/462
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Common Applications	https://www.oracle.com	A-ORA-COMM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Calendar product of Oracle E-Business Suite (component: Applications Calendar). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2114**	/security-alerts/cpujan2021.html	010221/463
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-	https://www.oracle.com/security-	A-ORA-COMM-010221/464

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Business Suite (component: Tasks). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2115**	alerts/cpujan2021.html	
customer_interaction_history					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business	https://www.oracle.com/security-	A-ORA-CUST-010221/465

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Suite (component: Outcome-Result). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2105**	alerts/cpujan2021.html	
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-CUST-010221/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2106**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10.	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-CUST-010221/467

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Customer Interaction History accessible data as well as unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2107**		
text					
Not Available	20-Jan-21	3.5	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-TEXT-010221/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Create Session privilege with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Text. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-2045**		
hyperion_infrastructure_technology					
Not Available	20-Jan-21	2.1	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 4.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-1993**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-HYPE-010221/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	3.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-1996**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-HYPE-010221/470
Not Available	20-Jan-21	1.2	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: RAS subsystems). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-HYPE-010221/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			human interaction from a person other than the attacker and while the vulnerability is in Oracle ZFS Storage Appliance Kit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2021-1999**		
retail_customer_management_and_segmentation_foundation					
Not Available	20-Jan-21	6.5	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Internal Operations). The supported version that is affected is 19.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Customer	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-RETA-010221/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management and Segmentation Foundation accessible data as well as unauthorized read access to a subset of Oracle Retail Customer Management and Segmentation Foundation accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Customer Management and Segmentation Foundation. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2021-2057**		
enterprise_repository					
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ENTE-010221/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/ UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-1994**		
agile_engineering_data_management					
Not Available	20-Jan-21	3.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/ UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-1996**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-AGIL-010221/474
server_bizlogic_script					
Not Available	20-Jan-21	4	Vulnerability in the Siebel Core - Server BizLogic Script product of Oracle Siebel CRM (component: Integration - Scripting). Supported versions that are affected are 20.12 and prior. Easily exploitable vulnerability allows low privileged	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-SERV-010221/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise Siebel Core - Server BizLogic Script. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel Core - Server BizLogic Script accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2004**		
enterprise_data_quality					
Not Available	20-Jan-21	4	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Proxy User Delegation). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle User Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2017**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ENTE-010221/476
retail_invoice_matching					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	4	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Proxy User Delegation). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle User Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2017**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-RETA-010221/477
user_management					
Not Available	20-Jan-21	4	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Proxy User Delegation). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-USER-010221/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle User Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2017**		
advanced_networking_option					
Not Available	20-Jan-21	5.1	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: CVE-2021-2018 affects Windows platform only. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2018**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ADVA-010221/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
adaptive_access_manager					
Not Available	20-Jan-21	5.1	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: CVE-2021-2018 affects Windows platform only. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2018**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ADAP-010221/480
enterprise_manager_for_fusion_applications					
Not Available	20-Jan-21	5.1	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Difficult to	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ENTE-010221/481

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: CVE-2021-2018 affects Windows platform only. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2018**		
rdbms_scheduler					
Not Available	20-Jan-21	6.5	Vulnerability in the RDBMS Scheduler component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Export Full Database privilege with network access via Oracle Net to compromise RDBMS Scheduler. Successful attacks	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-RDBM-010221/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in takeover of RDBMS Scheduler. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2035**		
peoplesoft_enterprise_fin_payables					
Not Available	20-Jan-21	4	Vulnerability in the PeopleSoft Enterprise FIN Payables product of Oracle PeopleSoft (component: Financial Sanctions). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Payables. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN Payables accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2021-2044**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-PEOP-010221/483
jd_edwards_enterpriseone_orchestrator					
Not Available	20-Jan-21	5	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards	https://www.oracle.com/security-alerts/cpuja	A-ORA-JD_E-010221/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: E1 IOT Orchestrator Security). The supported version that is affected is Prior to 9.2.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. While the vulnerability is in JD Edwards EnterpriseOne Orchestrator, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2021-2052**	n2021.html	
rdbms_sharding					
Not Available	20-Jan-21	6.5	Vulnerability in the RDBMS Sharding component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Any View, Create Any Trigger privilege with network access via Oracle Net to compromise RDBMS Sharding. Successful	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-RDBM-010221/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in takeover of RDBMS Sharding. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2054**		
complex_maintenance\,_repair\,_and_overhaul					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: Dialog Box). Supported versions that are affected are 11.5.10, 12.1 and 12.2. 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Complex Maintenance, Repair, and	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-COMP-010221/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Overhaul accessible data as well as unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2102**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: Dialog Box). Supported versions that are affected are 11.5.10, 12.1 and 12.2. 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Complex	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-COMP-010221/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Maintenance, Repair, and Overhaul accessible data as well as unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2103**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: Dialog Box). Supported versions that are affected are 11.5.10, 12.1 and 12.2. 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. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-COMP-010221/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2104**		
financial_services_revenue_management_and_billing					
Not Available	20-Jan-21	4	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: On Demand Billing). Supported versions that are affected are 2.9.0.0 and 2.9.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Revenue Management and Billing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Revenue Management and Billing accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-FINA-010221/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-2113**		
application_express_opportunity_tracker					
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle Application Express Opportunity Tracker component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Opportunity Tracker. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Opportunity Tracker, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Opportunity Tracker accessible data as well as unauthorized read access to a subset of Oracle Application Express Opportunity Tracker accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-APPL-010221/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-2116**		
application_express_survey_builder					
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle Application Express Survey Builder component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Survey Builder. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Survey Builder, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Survey Builder accessible data as well as unauthorized read access to a subset of Oracle Application Express Survey Builder accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-APPL-010221/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-2117**		
mysql					
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2009**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/492
Not Available	20-Jan-21	4.9	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Client. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2021-2010**		
Not Available	20-Jan-21	7.1	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2011**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/494
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-	A-ORA-MYSQ-010221/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2012**	alerts/cpujan2021.html	
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 5.7.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2014**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2016**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/497
Not Available	20-Jan-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2019**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2020**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/499
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2021**		
Not Available	20-Jan-21	6.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2022**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/501
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-	A-ORA-MYSQ-010221/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2024**	alerts/cpujan2021.html	
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2028**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2030**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/504
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/505

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2031**		
Not Available	20-Jan-21	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2032**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/506
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/507

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2036**		
Not Available	20-Jan-21	6.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2038**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/508
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported	https://www.oracle.com/security-alerts/cpuja	A-ORA-MYSQ-010221/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2065**	n2021.html	
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2070**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2072**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/511
Not Available	20-Jan-21	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2021-1998**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.30 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2001**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/513
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2002**		
Not Available	20-Jan-21	6.3	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2006**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/515

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	4.3	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2007**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/516
Not Available	20-Jan-21	2.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts).	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2042**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-2046**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/518
Not Available	20-Jan-21	7	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/519

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2021-2048**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2055**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/520

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	6.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2056**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/521
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts).	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2058**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2060**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/523
Not Available	20-Jan-21	6.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2061**		
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2076**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/525
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2081**		
Not Available	20-Jan-21	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2087**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/527
Not Available	20-Jan-21	4.9	Vulnerability in the MySQL	https://ww	A-ORA-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2088**	w.oracle.com/security-alerts/cpujan2021.html	MYSQ-010221/528
Not Available	20-Jan-21	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts).	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MYSQ-010221/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2122**		
outside_in_technology					
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-OUTS-010221/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L). **CVE ID : CVE-2021-2066**		
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-OUTS-010221/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L). **CVE ID : CVE-2021-2067**		
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-OUTS-010221/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L). **CVE ID : CVE-2021-2068**		
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). Supported versions that are affected are 8.5.4 and 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-OUTS-010221/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L). **CVE ID : CVE-2021-2069**		
argus_safety					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Argus Safety product of Oracle Health Sciences Applications (component: Case Form, Local Affiliate Form). The supported	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ARGU-010221/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version that is affected is 8.2.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Argus Safety. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Argus Safety accessible data as well as unauthorized read access to a subset of Oracle Argus Safety 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-2021-2040**		
Not Available	20-Jan-21	4	Vulnerability in the Oracle Argus Safety product of Oracle Health Sciences Applications (component: Letters). The supported version that is affected is 8.2.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Argus	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ARGU-010221/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Safety. While the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Argus Safety accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2021-2110**		
vm_virtualbox					
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-2073		
Not Available	20-Jan-21	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2074**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/537
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/538

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-2111**		
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/539

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-2112**		
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-2124**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/540
Not Available	20-Jan-21	3.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-2125**		
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/542

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-2086**		
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/543

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-2119**		
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-2120**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/544
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18.	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/545

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2021-2121**		
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products.	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/546

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2021-2123**		
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N). **CVE ID : CVE-2021-2126**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2127**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/548
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2021-2128**		
Not Available	20-Jan-21	3.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N). **CVE ID : CVE-2021-2129**		
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2021-2130**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/551
Not Available	20-Jan-21	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.18. Easily exploitable	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-VM_V-010221/552

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N). **CVE ID : CVE-2021-2131**		
database_server					
Not Available	20-Jan-21	2.1	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation,	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-DATA-010221/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 4.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-1993**		
Not Available	20-Jan-21	3.5	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having SYS Account privilege with network access via Oracle Net to compromise Unified Audit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Unified Audit accessible data. CVSS 3.1 Base Score 2.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2021-2000**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-DATA-010221/554
configurator					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: UI Servlet). Supported versions that are	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-CONF-010221/555

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data as well as unauthorized update, insert or delete access to some of Oracle Configurator accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2078**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: UI Servlet). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-CONF-010221/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data as well as unauthorized update, insert or delete access to some of Oracle Configurator accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2079**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Configurator product of Oracle Supply Chain (component: UI Servlet). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-CONF-010221/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while the vulnerability is in Oracle Configurator, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data as well as unauthorized update, insert or delete access to some of Oracle Configurator accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2080**		
business_intelligence_publisher					
Not Available	20-Jan-21	6.5	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update,	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/558

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2021-2013**		
Not Available	20-Jan-21	4.9	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Web Server). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update,	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2062**		
Not Available	20-Jan-21	6.5	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Administration). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-2049		
Not Available	20-Jan-21	6.5	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2021-2050**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/561
Not Available	20-Jan-21	6.5	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/562

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2021-2051**		
email_center					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-EMAI-010221/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2090**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-EMAI-010221/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2098**		
one-to-one_fulfillment					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products.	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ONE--010221/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2094**		
Not Available	20-Jan-21	6.4	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle One-to-One Fulfillment accessible data as well as unauthorized access to critical data or complete access to all One-to-One Fulfillment accessible	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ONE--010221/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-2100**		
Not Available	20-Jan-21	6.4	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle One-to-One Fulfillment accessible data as well as unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-2101**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ONE--010221/567
marketing					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Marketing product of Oracle	https://www.oracle.com	A-ORA-MARK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2026**	/security-alerts/cpujan2021.html	010221/568
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MARK-010221/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2027**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-MARK-010221/570

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2118**		
business_intelligence					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2025**		
Not Available	20-Jan-21	6.8	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Installation). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2041**		
Not Available	20-Jan-21	4.9	Vulnerability in the Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web Dashboards). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Business Intelligence Enterprise Edition accessible	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/573

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2021-2003**		
Not Available	20-Jan-21	4.3	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: BI Platform Security). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N).	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-BUSI-010221/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-2005		
crm_technical_foundation					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2084**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-CRM_-010221/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2085**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-CRM_-010221/576
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle CRM Technical Foundation	https://www.oracle.com	A-ORA-CRM_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2092**	/security-alerts/cpujan2021.html	010221/577
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component:	https://www.oracle.com/security-alerts/cpuja	A-ORA-CRM_-010221/578

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Preferences). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2099**	n2021.html	
istore					
Not Available	20-Jan-21	5	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Web interface). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ISTO-010221/579

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-2059**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ISTO-010221/580

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2077**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ISTO-010221/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2082**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Runtime Catalog). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2089**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ISTO-010221/582
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle iStore product of Oracle E-	https://www.oracle.com	A-ORA-ISTO-010221/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2096**	/security-alerts/cpujan2021.html	
common_applications					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are affected are 12.1.1-12.1.3 and	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-COMM-010221/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2093**		
data_integrator					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Worklist). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-DATA-010221/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Workflow, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Workflow accessible data as well as unauthorized update, insert or delete access to some of Oracle Workflow accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2015**		
Not Available	20-Jan-21	5.1	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-DATA-010221/586

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: CVE-2021-2018 affects Windows platform only. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2018**		
siebel_core_-_server_framework					
Not Available	20-Jan-21	4.9	Vulnerability in the Siebel Core - Server Framework product of Oracle Siebel CRM (component: Search). Supported versions that are affected are 20.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Core - Server Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Core - Server Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-SIEB-010221/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all Siebel Core - Server Framework accessible data as well as unauthorized update, insert or delete access to some of Siebel Core - Server Framework accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2039**		
isupport					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: User Responsibilities). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ISUP-010221/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2083**		
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Profile). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ISUP-010221/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2097**		
siebel_ui_framework					
Not Available	20-Jan-21	3.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-1996**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-SIEB-010221/590
workflow					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Worklist). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WORK-010221/591

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Workflow, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Workflow accessible data as well as unauthorized update, insert or delete access to some of Oracle Workflow accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2015**		
installed_base					
Not Available	20-Jan-21	4.3	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: APIs). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-INST-010221/592

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2021-2023**		
weblogic_server					
Not Available	20-Jan-21	5.1	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/593

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking Option. Note: CVE-2021-2018 affects Windows platform only. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2018**		
Not Available	20-Jan-21	4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2021-2033**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/594
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). The supported version that is affected is	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2064**		
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2075**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Not Available	20-Jan-21	6.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2109**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/597
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/598

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-1994**		
Not Available	20-Jan-21	4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-1995**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/599
Not Available	20-Jan-21	3.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/600

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2021-1996**		
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2047**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-WEBL-010221/601
Not Available	20-Jan-21	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware	https://www.oracle.com/security-	A-ORA-WEBL-010221/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: Core Components). The supported version that is affected is 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2108**	alerts/cpujan2021.html	
hospitality_reporting_and_analytics					
Not Available	20-Jan-21	5.5	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Report). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-HOSP-010221/603

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2021-1997**		
hospitality_simphony					
Not Available	20-Jan-21	5.1	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Advanced Networking Option, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Advanced Networking Option. Note: CVE-2021-2018 affects Windows platform only. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-HOSP-010221/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2021-2018**		
peoplesoft_enterprise_peopletools					
Not Available	20-Jan-21	4.6	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2063**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-PEOP-010221/605
Not Available	20-Jan-21	6.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.56, 8.57 and	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-PEOP-010221/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.58. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2071**		
Not Available	20-Jan-21	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-PEOP-010221/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools 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-2021-2043**		
enterprise_manager_ops_center					
Not Available	20-Jan-21	5.8	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Worklist). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Workflow, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Workflow accessible data as well as	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ENTE-010221/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle Workflow accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2021-2015**		
Not Available	20-Jan-21	2.1	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 4.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2021-1993**	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ENTE-010221/609
Not Available	20-Jan-21	1.2	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: RAS subsystems). The supported version that is affected is 8.8.	https://www.oracle.com/security-alerts/cpujan2021.html	A-ORA-ENTE-010221/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle ZFS Storage Appliance Kit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2021-1999**		
phpgurukul					
daily_expense_tracker_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-21	4.3	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS via the user-profile.php Full Name field. **CVE ID : CVE-2021-26303**	N/A	A-PHP-DAIL-010221/611
phpgurukul_daily_expense_tracker_system_project					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
phpgurukul_daily_expense_tracker_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-21	4.3	PHPGurukul Daily Expense Tracker System 1.0 is vulnerable to stored XSS via the add-expense.php Item parameter. **CVE ID : CVE-2021-26304**	N/A	A-PHP-PHPG-010221/612
Prestashop					
prestashop					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-21	7.5	The store system in PrestaShop 1.7.7.0 allows time-based boolean SQL injection via the module=productcomments controller=CommentGrade id_products[] parameter. **CVE ID : CVE-2021-3110**	N/A	A-PRE-PRES-010221/613
pysaml2_project					
pysaml2					
Improper Verification of Cryptographic Signature	21-Jan-21	4.3	PySAML2 is a pure python implementation of SAML Version 2 Standard. PySAML2 before 6.5.0 has an improper verification of cryptographic signature vulnerability. All users of pysaml2 that need to validate signed SAML documents are impacted. The vulnerability is a variant of XML Signature wrapping because it did not validate the SAML document against an XML schema. This allowed invalid XML documents to be processed and such a document can trick pysaml2	https://github.com/IdentityPython/pysaml2/commit/1d8fd268f5bf887480a403a7a5ef8f048157cc14 , https://github.com/IdentityPython/pysaml2/security/advisories/GHSA-f4g9-h89h-	A-PYS-PYSA-010221/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with a wrapped signature. This is fixed in PySAML2 6.5.0. **CVE ID : CVE-2021-21238**	jgv9	
Improper Verification of Cryptographic Signature	21-Jan-21	4.3	PySAML2 is a pure python implementation of SAML Version 2 Standard. PySAML2 before 6.5.0 has an improper verification of cryptographic signature vulnerability. Users of pysaml2 that use the default CryptoBackendXmlSec1 backend and need to verify signed SAML documents are impacted. PySAML2 does not ensure that a signed SAML document is correctly signed. The default CryptoBackendXmlSec1 backend is using the xmlsec1 binary to verify the signature of signed SAML documents, but by default xmlsec1 accepts any type of key found within the given document. xmlsec1 needs to be configured explicitly to only use only _x509 certificates_ for the verification process of the SAML document signature. This is fixed in PySAML2 6.5.0. **CVE ID : CVE-2021-21239**	https://github.com/IdentityPython/pysaml2/commit/46578df0695269a16f1c94171f1429873f90ed99, https://github.com/IdentityPython/pysaml2/security/advisories/GHSA-5p3x-r448-pc62	A-PYS-PYSA-010221/615
Python					
python					
Buffer Copy without Checking	19-Jan-21	7.5	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in	https://bugs.python.org/issue42938,	A-PYT-PYTH-010221/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			_ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely. **CVE ID : CVE-2021-3177**	https://github.com/python/cpython/pull/24239, https://python-security.readthedocs.io/vuln/ctypes-buffer-overflow-pycarg_repr.html	
report_project					
report					
Cross-Site Request Forgery (CSRF)	25-Jan-21	4.3	The MediaWiki "Report" extension has a Cross-Site Request Forgery (CSRF) vulnerability. Before fixed version, there was no protection against CSRF checks on Special:Report, so requests to report a revision could be forged. The problem has been fixed in commit f828dc6 by making use of MediaWiki edit tokens. **CVE ID : CVE-2021-21275**	https://github.com/Kenny2github/Report/commit/f828dc6f73cdfaea5639edbf8ac7b326eeefb117, https://github.com/Kenny2github/Report/security/advisories/GHSA-9f3w-c334-jm2h	A-REP-REPO-010221/617
Revive-adserver					
revive_adserver					
Improper Neutralization of Input During Web Page Generation	28-Jan-21	4.3	Revive Adserver before 5.1.1 is vulnerable to a reflected XSS vulnerability in userlog-index.php via the `period_preset` parameter.	https://github.com/revive-adserver/revive-adserver/co	A-REV-REVI-010221/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2021-22874**	mmit/e2a67ce8, https://www.revive-adserver.com/security/revive-sa-2021-002/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jan-21	4.3	Revive Adserver before 5.1.1 is vulnerable to a reflected XSS vulnerability in stats.php via the `setPerPage` parameter. **CVE ID : CVE-2021-22875**	https://github.com/revive-adserver/revive-adserver/commit/6f46076a, https://www.revive-adserver.com/security/revive-sa-2021-002/	A-REV-REVI-010221/619
spotweb_project					
spotweb					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Jan-21	7.5	SQL injection exists in Spotweb 1.4.9 because the notAllowedCommands protection mechanism is inadequate, e.g., a variation of the payload may be used. NOTE: this issue exists because of an incomplete fix for CVE-2020-35545. **CVE ID : CVE-2021-3286**	N/A	A-SPO-SPOT-010221/620
the-guild					
graphql-tools					
Improper Neutralizatio	20-Jan-21	7.5	This affects the package @graphql-tools/git-loader	https://github.com/arda	A-THE-GRAP-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			before 6.2.6. The use of exec and execSync in packages/loaders/git/src/load-git.ts allows arbitrary command injection. **CVE ID : CVE-2021-23326**	tan/graphql-tools/commit/6a966beee8ca8b2f4adfe93318b96e4a5c501eac, https://github.com/ardatan/graphql-tools/pull/2470	010221/621
weseek					
growi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-21	4.3	Cross-site scripting vulnerability in GROWI (v4.2 Series) versions prior to v4.2.3 allows remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20619**	https://weseek.co.jp/security/2021/01/18/vulnerability/growi-prevent-xss4/	A-WES-GROW-010221/622
Xwiki					
Xwiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-21	3.5	XWiki 12.10.2 allows XSS via an SVG document to the upload feature of the comment section. **CVE ID : CVE-2021-3137**	N/A	A-XWI-XWIK-010221/623