EUVD Vulnerability Report

Search in report... | Filter by Vendor | Filter by Product | All CVSS | Export PDF

EUVD_ID	Alt_IDs	Exploitation	CVSS	EPSS	Product	Vendor	Changed	Summary	Version	Published	Updated	
EUVD-2025-14705	CVE-2025-32756,	Not available	v3.1: 9.6	0.14	FortiCamera, FortiCamera, FortiNDR, FortiCamera, FortiNDR, FortiMail, FortiNDR, FortiNDR, FortiNDR, FortiMail, FortiVoice, FortiMail, FortiVoice, FortiNDR, FortiVoice, FortiRecorder, FortiRecorder, FortiNDR, FortiNDR, FortiNDR, FortiRecorder, FortiNDR, FortiMail	Fortinet	May 14, 2025, 10:20:22 PM	A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiVoice versions 7.2.0, 7.0.0 through 7.0.6, 6.4.0 through 6.4.10, FortiRecorder versions 7.2.0 through 7.2.3, 7.0.0 through 7.0.5, 6.4.0 through 6.4.5, FortiMail versions 7.6.0 through 7.6.2, 7.4.0 through 7.4.4, 7.2.0 through 7.2.7, 7.0.0 through 7.0.8, FortiNDR versions 7.6.0, 7.4.0 through 7.4.7, 7.2.0 through 7.2.4, 7.0.0 through 7.0.6, FortiCamera versions 2.1.0 through 2.1.3, 2.0 all versions, 1.1 all versions, allows a remote unauthenticated attacker to execute arbitrary code or commands via sending HTTP requests with specially crafted hash cookie.	1.1.0 ≤1.1.5, 2.1.0 ≤2.1.3, 7.6.0, 2.0.0, 1.5.0 ≤1.5.3, 7.6.0 ≤7.6.2, 7.2.0 ≤7.2.4, 7.0.0 ≤7.0.6, 1.2.0, 7.2.0 ≤7.2.7, 6.4.0 ≤6.4.10, 7.4.0 ≤7.4.4, 7.2.0, 7.4.0 ≤7.4.7, 7.0.0 ≤7.0.6, 6.4.0 ≤6.4.5, 7.2.0 ≤7.2.3, 7.1.0 ≤7.1.1, 1.3.0 ≤1.3.1, 1.4.0, 7.0.0 ≤7.0.5, 1.1.0, 7.0.0 ≤7.0.8	May 13, 2025, 2:46:44 PM	May 14, 2025, 10:20:22 PM	http
EUVD-2024-54503	CVE-2024-35281,	Not available	v3.1: 2.3	0.0	FortiClientMac, FortiClientMac, FortiVoiceUCDesktop, FortiClientMac	Fortinet	May 13, 2025, 3:17:58 PM	An improper isolation or compartmentalization vulnerability [CWE-653] in FortiClientMac version 7.4.2 and below, version 7.2.8 and below, 7.0 all versions and FortiVoiceUCDesktop 3.0 all versions desktop application may allow an authenticated attacker to inject code via Electron environment variables.	7.4.0 ≤7.4.2, 7.2.0 ≤7.2.8, 3.0.0 ≤3.0.16, 7.0.0 ≤7.0.14	May 13, 2025, 2:46:42 PM	May 13, 2025, 3:17:58 PM	http
EUVD-2025-14956	CVE-2025-22859,	Not available	v3.1: 5.0	0.0	FortiClientEMS	Fortinet	May 13, 2025, 3:17:40 PM	A Relative Path Traversal vulnerability [CWE-23] in FortiClientEMS 7.4.0 through 7.4.1 and FortiClientEMS Cloud 7.4.0 through 7.4.1 may allow a remote unauthenticated attacker to perform a limited arbitrary file write on the system via upload requests.	7.4.0 ≤7.4.1	May 13, 2025, 2:46:42 PM	May 13, 2025, 3:17:40 PM	http
EUVD-2024-20636	CVE-2024-23111, GSD-2024-23111,	Not available	v3.1: 6.2	0.04	FortiProxy, FortiProxy, FortiOS, FortiOS, FortiProxy, FortiOS	Fortinet	May 1, 2025, 3:55:29 AM	An improper neutralization of input during web page Generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions reboot page	7.2.0 ≤7.2.8, 7.4.0 ≤7.4.2, 7.0.0 ≤7.0.13, 7.4.0 ≤7.4.2, 7.0.0 ≤7.0.14, 7.2.0 ≤7.2.6	Jun 11, 2024, 2:32:00 PM	May 1, 2025, 3:55:29 AM	http

								may allow a remote privileged attacker with super-admin access to execute JavaScript code via crafted HTTP GET requests.				
EUVD-2024-23306	CVE-2024-26010, GSD-2024-26010,	Not available	v3.1: 6.7	0.07	FortiProxy, FortiOS, FortiSwitchManager, FortiOS, FortiPAM, FortiProxy, FortiOS, FortiOS, FortiProxy, FortiProxy, FortiOS, FortiSwitchManager, FortiProxy, FortiPAM, FortiOS, FortiProxy, FortiPAM, FortiProxy	Fortinet	May 1, 2025, 3:55:28 AM	A stack-based buffer overflow in Fortinet FortiPAM version 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiWeb, FortiAuthenticator, FortiSwitchManager version 7.2.0 through 7.2.3, 7.0.1 through 7.0.3, FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15, 6.2.0 through 6.2.16, 6.0.0 through 6.0.18, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.15, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specially crafted packets.	7.0.0 ≤7.0.15, 6.2.0 ≤6.2.16, 7.0.1 ≤7.0.3, 7.0.0 ≤7.0.14, 1.2.0, 1.0.0 ≤1.0.7, 6.0.0 ≤6.0.18, 7.4.0 ≤7.4.3, 1.1.0 ≤1.1.6, 7.2.0 ≤7.2.9, 6.4.0 ≤6.4.15, 7.2.0 ≤7.2.3, 1.2.0 ≤1.2.13, 1.1.0 ≤1.1.2, 7.2.0 ≤7.2.7, 7.4.0 ≤7.4.2, 1.0.0 ≤1.0.3, 2.0.0 ≤2.0.13	Jun 11, 2024, 2:32:03 PM	May 1, 2025, 3:55:28 AM	http
EUVD-2024-19368	CVE-2024-21754, GSD-2024-21754,	Not available	v3.1: 1.7	0.36	FortiProxy, FortiOS, FortiProxy, FortiProxy, FortiOS, FortiOS, FortiOS, FortiProxy	Fortinet	May 1, 2025, 3:55:28 AM	A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file.	7.2.0 ≤7.2.10, 7.4.0 ≤7.4.3, 2.0.0 ≤2.0.14, 7.0.0 ≤7.0.17, 7.0.0 ≤7.0.15, 7.2.0 ≤7.2.8, 6.4.0 ≤6.4.15, 7.4.0 ≤7.4.2	Jun 11, 2024, 2:32:01 PM	May 1, 2025, 3:55:28 AM	http
EUVD-2023-50904	CVE-2023-46720, GSD-2023-46720,	Not available	v3.1: 6.3	0.03	FortiOS, FortiOS, FortiOS, FortiOS, FortiOS, FortiOS	Fortinet	May 1, 2025, 3:55:28 AM	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.12 and 6.4.6 through 6.4.15 and 6.2.9 through 6.2.16 and 6.0.13 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted CLI commands.	7.2.0 ≤7.2.7, 6.2.9 ≤6.2.16, 7.0.0 ≤7.0.12, 6.0.13 ≤6.0.18, 7.4.0 ≤7.4.1, 6.4.6 ≤6.4.15	Jun 11, 2024, 2:32:00 PM	May 1, 2025, 3:55:28 AM	http
EUVD-2024-20633	CVE-2024-23108, GSD-2024-23108,	Not available	v3.1: 9.7	89.79	FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM	Fortinet	Apr 24, 2025, 3:54:48 PM	An improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 7.1.0 through 7.1.1 and 7.0.0 through 7.0.2 and 6.7.0 through 6.7.8 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.2 and 6.4.0 through 6.4.2 allows attacker to execute unauthorized code or commands via via crafted API requests.	6.7.0 ≤6.7.8, 6.6.0 ≤6.6.3, 7.0.0 ≤7.0.2, 7.1.0 ≤7.1.1, 6.5.0 ≤6.5.2	Feb 5, 2024, 1:26:15 PM	Apr 24, 2025, 3:54:48 PM	http

EUVD-2024-19376	CVE-2024-21762, GSD-2024-21762,	Not available	v3.1: 9.6	92.23	FortiOS, FortiOS, FortiProxy, FortiProxy, FortiOS, FortiOS, FortiProxy, FortiProxy, FortiOS, FortiProxy, FortiProxy, FortiOS, FortiProxy, FortiOS, FortiProxy	Fortinet	Apr 24, 2025, 3:49:22 PM	A out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specifically crafted requests	7.2.0 ≤7.2.6, 6.2.0 ≤6.2.15, 7.0.0 ≤7.0.14, 1.1.0 ≤1.1.6, 7.0.0 ≤7.0.13, 1.0.0 ≤1.0.7, 6.4.0 ≤6.4.14, 7.2.0 ≤7.2.8, 7.4.0 ≤7.4.2, 7.4.0 ≤7.4.2, 1.2.0 ≤1.2.13, 6.0.0 ≤6.0.17, 2.0.0 ≤2.0.13	Feb 9, 2024, 8:14:25 AM	Apr 24, 2025, 3:49:22 PM	http
EUVD-2023-41785	CVE-2023-37932, GSD-2023-37932,	Not available	v3.1: 6.2	0.48	FortiVoice, FortiVoice, FortiVoice	Fortinet	Apr 17, 2025, 3:45:35 PM	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability [CWE-22] in FortiVoiceEntreprise version 7.0.0 and before 6.4.7 allows an authenticated attacker to read arbitrary files from the system via sending crafted HTTP or HTTPS requests	6.0.0 ≤6.0.12, 6.4.0 ≤6.4.7, 7.0.0	Jan 10, 2024, 5:48:00 PM	Apr 17, 2025, 3:45:35 PM	http
EUVD-2025-10266	CVE-2024-48887, GHSA-w84w-59g8-pmg9,	Not available	v3.1: 9.3	0.08	FortiSwitch, FortiSwitch, FortiSwitch, FortiSwitch, FortiSwitch	Fortinet	Apr 8, 2025, 5:49:20 PM	A unverified password change vulnerability in Fortinet FortiSwitch GUI may allow a remote unauthenticated attacker to change admin passwords via a specially crafted request	7.2.0 ≤7.2.8, 7.0.0 ≤7.0.10, 7.4.0 ≤7.4.4, 6.4.0 ≤6.4.14, 7.6.0	Apr 8, 2025, 4:52:02 PM	Apr 8, 2025, 5:49:20 PM	http http
EUVD-2025-10301	CVE-2025-22855, GHSA-962v-6x3f-5mw4,	Not available	v3.1: 2.6	0.04	FortiClientEMS, FortiClientEMS	Fortinet	Apr 8, 2025, 2:47:47 PM	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in Fortinet FortiClient before 7.4.1 may allow the EMS administrator to send messages containing javascript code.	7.2.1 ≤7.2.8, 7.4.0 ≤7.4.1	Apr 8, 2025, 2:02:44 PM	Apr 8, 2025, 2:47:47 PM	http http
EUVD-2025-10300	CVE-2025-25254, GHSA-q7jr-v677-ww76,	Not available	v3.1: 6.8	0.08	FortiWeb, FortiWeb, FortiWeb, FortiWeb	Fortinet	Apr 8, 2025, 2:44:39 PM	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in FortiWeb version 7.6.2 and below, version 7.4.6 and below, 7.2 all versions, 7.0 all versions endpoint may allow an authenticated admin to access and modify the filesystem via crafted requests.	7.6.0 ≤7.6.2, 7.4.0 ≤7.4.6, 7.2.0 ≤7.2.11, 7.0.0 ≤7.0.11	Apr 8, 2025, 2:02:44 PM	Apr 8, 2025, 2:44:39 PM	http http
EUVD-2025-10304	CVE-2024-54025, GHSA-jr95-cvrj-r656,	Not available	v3.1: 6.5	0.06	FortiIsolator	Fortinet	Apr 8, 2025, 2:41:17 PM	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiIsolator CLI before version 2.4.6 allows a privileged attacker to execute unauthorized code or commands via	2.4.3 ≤2.4.6	Apr 8, 2025, 2:02:45 PM	Apr 8, 2025, 2:41:17 PM	http http

								crafted CLI requests.				
EUVD-2025-10308	CVE-2024-54024, GHSA-83g9-r3gv-pq9c,	Not available	v3.1: 7.0	0.32	FortiIsolator	Fortinet	Apr 8, 2025, 2:37:57 PM	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiIsolator before version 2.4.6 allows a privileged attacker with super-admin profile and CLI access to execute unauthorized code via specifically crafted HTTP requests.	2.4.3 ≤2.4.6	Apr 8, 2025, 2:02:45 PM	Apr 8, 2025, 2:37:57 PM	http http
EUVD-2024-29943	CVE-2024-32122, GSD-2024-32122,	Not available	v3.1: 2.1	0.02	FortiOS, FortiOS, FortiOS, FortiOS	Fortinet	Apr 8, 2025, 2:32:01 PM	A storing passwords in a recoverable format in Fortinet FortiOS versions 7.2.0 through 7.2.1 allows attacker to information disclosure via modification of LDAP server IP to point to a malicious server.	6.4.0 ≤6.4.16, 7.4.0 ≤7.4.7, 7.2.0 ≤7.2.11, 7.0.0 ≤7.0.17	Apr 8, 2025, 2:02:57 PM	Apr 8, 2025, 2:32:01 PM	http http
EUVD-2025-10307	CVE-2024-46671, GHSA-cwrm-9wh5-jq4m,	Not available	v3.1: 5.6	0.05	FortiWeb, FortiWeb, FortiWeb, FortiWeb	Fortinet	Apr 8, 2025, 2:30:24 PM	An Incorrect User Management vulnerability [CWE-286] in FortiWeb version 7.6.2 and below, version 7.4.6 and below, version 7.2.10 and below, version 7.0.11 and below widgets dashboard may allow an authenticated attacker with at least read-only admin permission to perform operations on the dashboard of other administrators via crafted requests.	7.2.0 ≤7.2.10, 7.0.0 ≤7.0.11, 7.4.0 ≤7.4.6, 7.6.0 ≤7.6.2	Apr 8, 2025, 2:02:59 PM	Apr 8, 2025, 2:30:24 PM	http http
EUVD-2025-10306	CVE-2024-52962, GHSA-j27p-5p5f-gjjv,	Not available	v3.1: 5.0	0.05	FortiManager, FortiManager, FortiManager, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiAnalyzer, FortiAnalyzer	Fortinet	Apr 8, 2025, 2:27:48 PM	An Improper Output Neutralization for Logs vulnerability [CWE-117] in FortiAnalyzer version 7.6.1 and below, version 7.4.5 and below, version 7.2.8 and below, version 7.0.13 and below and FortiManager version 7.6.1 and below, version 7.4.5 and below, version 7.2.8 and below, version 7.0.12 and below may allow an unauthenticated remote attacker to pollute the logs via crafted login requests.	7.0.0 ≤7.0.13, 7.6.0 ≤7.6.1, 7.2.0 ≤7.2.8, 7.2.0 ≤7.2.8, 7.4.0 ≤7.4.5, 7.0.0 ≤7.0.13, 7.4.0 ≤7.4.5, 7.6.0 ≤7.6.1	Apr 8, 2025, 2:03:34 PM	Apr 8, 2025, 2:27:48 PM	http http
EUVD-2023-41783	CVE-2023-37930, GSD-2023-37930,	Not available	v3.1: 6.7	0.11	FortiProxy, FortiProxy, FortiOS, FortiOS, FortiOS, FortiOS	Fortinet	Apr 8, 2025, 2:27:09 PM	Multiple issues including the use of uninitialized ressources [CWE-908] and excessive iteration [CWE-834] vulnerabilities in Fortinet FortiOS SSL VPN webmode version 7.4.0, version 7.2.0 through 7.2.5, version 7.0.1 through 7.0.11 and version 6.4.7 through 6.4.14 and Fortinet FortiProxy SSL VPN webmode version 7.2.0 through 7.2.6 and version 7.0.0 through 7.0.12 allows a VPN user to corrupt memory potentially leading to code or commands execution via specifically crafted requests.	7.2.0 ≤7.2.6, 7.0.0 ≤7.0.12, 6.4.7 ≤6.4.14, 7.4.0, 7.0.1 ≤7.0.11, 7.2.0 ≤7.2.5	Apr 8, 2025, 2:03:38 PM	Apr 8, 2025, 2:27:09 PM	http http

EUVD-2024-23309	CVE-2024-26013, GSD-2024-26013,	Not available	v3.1: 7.1	0.06	FortiManager, FortiManager, FortiOS, FortiProxy, FortiManager, FortiProxy, FortiOS, FortiManager, FortiManager, FortiOS, FortiProxy, FortiProxy, FortiOS, FortiOS	Fortinet	Apr 8, 2025, 2:24:44 PM	A improper restriction of communication channel to intended endpoints vulnerability [CWE-923] in Fortinet FortiOS version 7.4.0 through 7.4.4, 7.2.0 through 7.2.8, 7.0.0 through 7.0.15, 6.4.0 through 6.4.15 and before 6.2.16, Fortinet FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9 and before 7.0.15, Fortinet FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and before 6.2.13, Fortinet FortiAnalyzer version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and before 6.2.13, Fortinet FortiVoice version 7.0.0 through 7.0.2 before 6.4.8 and Fortinet FortiWeb before 7.4.2 may allow an unauthenticated attacker in a man-in-the-middle position to impersonate the management device (FortiCloud server or/and in certain conditions, FortiManager), via intercepting the FGFM authentication request between the management device and the managed device	6.4.0 ≤6.4.14, 7.0.0 ≤7.0.11, 6.2.0 ≤6.2.16, 7.4.0 ≤7.4.2, 6.2.0 ≤6.2.13, 7.2.0 ≤7.2.9, 6.4.0 ≤6.4.15, 7.4.0 ≤7.4.2, 7.2.0 ≤7.2.4, 7.0.0 ≤7.0.14, 2.0.0 ≤2.0.14, 7.0.0 ≤7.0.15, 7.4.0 ≤7.4.3, 7.2.0 ≤7.2.7	Apr 8, 2025, 2:03:49 PM	Apr 8, 2025, 2:24:44 PM	http http
EUVD-2025-10305	CVE-2024-50565, GHSA-j94p-gv3v-cg5q,	Not available	v3.1: 3.0	0.07	FortiAnalyzer, FortiWeb, FortiOS, FortiVoice, FortiAnalyzer, FortiAnalyzer, FortiWeb, FortiOS, FortiVoice, FortiOS, FortiWeb, FortiAnalyzer, FortiVoice, FortiOS, FortiAnalyzer, FortiOS	Fortinet	Apr 8, 2025, 2:22:56 PM	A improper restriction of communication channel to intended endpoints vulnerability [CWE-923] in Fortinet FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15 and 6.2.0 through 6.2.16, Fortinet FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.15 and 2.0.0 through 2.0.14, Fortinet FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and 6.2.0 through 6.2.13, Fortinet FortiAnalyzer version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14 and 6.2.0 through 6.2.13, Fortinet FortiVoice version 7.0.0 through 7.0.2, 6.4.0 through 6.4.8 and 6.0.0 through 6.0.12 and Fortinet FortiWeb version 7.4.0 through 7.4.2, 7.2.0 through 7.2.10, 7.0.0 through 7.0.10 allows an unauthenticated attacker in a man-in-the-middle position to impersonate the management device (FortiCloud server or/and in certain conditions,	6.4.0 ≤6.4.14, 7.2.0 ≤7.2.11, 7.2.0 ≤7.2.8, 7.0.0 ≤7.0.2, 7.2.0 ≤7.2.4, 7.4.0 ≤7.4.2, 7.0.0 ≤7.0.11, 7.0.0 ≤7.0.15, 6.4.0 ≤6.4.8, 6.4.0 ≤6.4.16, 7.4.0 ≤7.4.2, 7.0.0 ≤7.0.11, 6.0.0 ≤6.0.12, 6.2.0 ≤6.2.16, 6.2.0 ≤6.2.13, 7.4.0 ≤7.4.4	Apr 8, 2025, 2:03:51 PM	Apr 8, 2025, 2:22:56 PM	http http

								FortiManager), via intercepting the FGFM authentication request between the management device and the managed device				
EUVD-2023-45268	CVE-2023-40714, GSD-2023-40714,	Not available	v3.1: 9.7	0.35	FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM	Fortinet	Apr 2, 2025, 4:16:37 PM	A relative path traversal in Fortinet FortiSIEM versions 7.0.0, 6.7.0 through 6.7.2, 6.6.0 through 6.6.3, 6.5.1, 6.5.0 allows attacker to escalate privilege via uploading certain GUI elements	6.7.0 ≤6.7.2, 6.6.0 ≤6.6.3, 6.5.0 ≤6.5.1, 7.0.0	Apr 2, 2025, 8:06:48 AM	Apr 2, 2025, 4:16:37 PM	http
EUVD-2021-12926	CVE-2021-26105, GSD-2021-26105,	Not available	v3.1: 6.4	0.0	FortiSandbox, FortiSandbox	Fortinet	Mar 31, 2025, 6:19:39 PM	A stack-based buffer overflow vulnerability (CWE-121) in the profile parser of FortiSandbox version 3.2.2 and below, version 3.1.4 and below may allow an authenticated attacker to potentially execute unauthorized code or commands via specifically crafted HTTP requests.	3.1.4, 3.2.2	Mar 24, 2025, 3:27:56 PM	Mar 31, 2025, 6:19:39 PM	http http
EUVD-2023-37465	CVE-2023-33302, GSD-2023-33302,	Not available	v3.1: 4.5	0.09	FortiMail, FortiMail, FortiMail, FortiMail, FortiNDR, FortiMail, FortiNDR, FortiNDR, FortiMail, FortiNDR, FortiNDR, FortiMail, FortiNDR, FortiNDR, FortiNDR, FortiMail, FortiMail	Fortinet	Mar 31, 2025, 3:30:12 PM	A buffer copy without checking size of input ('classic buffer overflow') in Fortinet FortiMail webmail and administrative interface version 6.4.0 through 6.4.4 and before 6.2.6 and FortiNDR administrative interface version 7.2.0 and before 7.1.0 allows an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests.	5.2.0 ≤5.2.10, 6.2.0 ≤6.2.6, 5.0.0 ≤5.0.11, 6.0.0 ≤6.0.10, 1.4.0, 5.4.0 ≤5.4.12, 1.5.0 ≤1.5.3, 1.1.0, 5.3.0 ≤5.3.10, 7.0.0 ≤7.0.6, 7.1.0, 5.3.12 ≤5.3.13, 1.2.0, 7.2.0, 1.3.0 ≤1.3.1, 5.1.0 ≤5.1.7, 6.4.0 ≤6.4.4	Mar 31, 2025, 2:58:11 PM	Mar 31, 2025, 3:30:12 PM	http http
EUVD-2025-8613	CVE-2019-16149, GHSA-j8c2-6298-q92j,	Not available	v3.1: 5.4	0.0	FortiClientEMS	Fortinet	Mar 28, 2025, 2:30:50 PM	An Improper Neutralization of Input During Web Page Generation in FortiClientEMS version 6.2.0 may allow a remote attacker to execute unauthorized code by injecting malicious payload in the user profile of a FortiClient instance being managed by the vulnerable system.	6.2.0	Mar 28, 2025, 9:07:30 AM	Mar 28, 2025, 2:30:50 PM	http http
EUVD-2021-10928	CVE-2021-24008, GSD-2021-24008,	Not available	v3.1: 5.0	0.08	FortiDDoS, FortiDDoS-CM, FortiDDoS, FortiDDoS, FortiDDoS-CM, FortiDDoS, FortiDDoS-CM, FortiDDoS-CM, FortiNDR, FortiDDoS, FortiNDR, FortiNDR, FortiDDoS-CM, FortiDDoS, FortiDDoS, FortiDDoS, FortiDDoS, FortiNDR, FortiNDR	Fortinet	Mar 28, 2025, 1:39:11 PM	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiDDoS version 5.4.0, version 5.3.2 and below, version 5.2.0, version 5.1.0, version 5.0.0, version 4.7.0, version 4.6.0, version 4.5.0, version 4.4.2 and below, FortiDDoS-CM version 5.3.0, version 5.2.0, version 5.1.0, version 5.0.0, version 4.7.0, FortiVoice version 6.0.6 and below, FortiRecorder version 6.0.3 and	5.4.0, 5.0.0, 5.2.0, 4.7.0, 5.3.0, 4.6.0, 4.7.0, 5.1.0, 1.5.0 ≤1.5.3, 4.4.0 ≤4.4.2, 1.4.0, 1.1.0, 5.2.0, 5.0.0, 5.3.0 ≤5.3.2, 4.5.0, 5.1.0, 1.3.0 ≤1.3.1,	Mar 28, 2025, 10:13:32 AM	Mar 28, 2025, 1:39:11 PM	http http

								below and FortiMail version 6.4.1 and below, version 6.2.4 and below, version 6.0.9 and below may allow a remote, unauthenticated attacker to obtain potentially sensitive software-version information by reading a JavaScript file.	1.2.0			
EUVD-2023-29551	CVE-2023-25610, GSD-2023-25610,	Not available	v3.1: 9.3	9.77	FortiOS, FortiOS, FortiOS-6K7K, FortiOS, FortiProxy, FortiProxy, FortiOS-6K7K, FortiAnalyzer, FortiOS, FortiManager, FortiWeb, FortiAnalyzer, FortiAnalyzer, FortiWeb, FortiOS-6K7K, FortiOS-6K7K, FortiProxy, FortiWeb, FortiManager, FortiManager, FortiWeb, FortiOS-6K7K, FortiOS, FortiWeb, FortiProxy, FortiManager, FortiOS-6K7K, FortiManager, FortiWeb, FortiOS, FortiOS-6K7K, FortiOS-6K7K, FortiOS-6K7K, FortiSwitchManager, FortiOS, FortiAnalyzer, FortiProxy, FortiAnalyzer, FortiOS, FortiOS, FortiOS-6K7K, FortiSwitchManager	Fortinet	Mar 24, 2025, 6:42:44 PM	A buffer underwrite ('buffer underflow') vulnerability in the administrative interface of Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.6, version 6.4.0 through 6.4.11 and version 6.2.12 and below, FortiProxy version 7.2.0 through 7.2.2, version 7.0.0 through 7.0.8, version 2.0.12 and below and FortiOS-6K7K version 7.0.5, version 6.4.0 through 6.4.10 and version 6.2.0 through 6.2.10 and below allows a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.	6.0.0 ≤6.0.18, 5.2.0 ≤5.2.15, 7.0.5, 6.4.0 ≤6.4.11, 7.0.0 ≤7.0.8, 2.0.0 ≤2.0.14, 6.0.12 ≤6.0.18, 6.0.0 ≤6.0.11, 5.0.0 ≤5.0.14, 6.0.0 ≤6.0.11, 6.2.0 ≤6.2.7, 7.0.0 ≤7.0.4, 6.4.0 ≤6.4.11, 6.4.0 ≤6.4.2, 6.4.10, 6.2.6 ≤6.2.7, 1.2.0 ≤1.2.13, 7.2.0 ≤7.2.1, 7.0.0 ≤7.0.4, 6.4.0 ≤6.4.11, 6.1.0 ≤6.1.3, 6.4.8, 5.4.0 ≤5.4.13, 7.0.0 ≤7.0.6, 7.2.0 ≤7.2.2, 7.2.0, 6.4.6, 6.2.0 ≤6.2.10, 6.3.0 ≤6.3.22, 6.2.0 ≤6.2.12, 6.0.10, 6.2.9 ≤6.2.12, 6.2.4, 7.2.0 ≤7.2.1, 7.2.0 ≤7.2.3, 7.2.0, 1.1.0 ≤1.1.6, 6.2.0 ≤6.2.10, 7.0.0 ≤7.0.9, 5.6.0 ≤5.6.14, 6.4.2, 7.0.0 ≤7.0.1	Mar 24, 2025, 3:39:48 PM	Mar 24, 2025, 6:42:44 PM	http http
EUVD-2021-12912	CVE-2021-26091, GSD-2021-26091,	Not available	v3.1: 6.9	0.04	FortiMail, FortiMail, FortiMail	Fortinet	Mar 24, 2025, 6:31:01 PM	A use of a cryptographically weak pseudo-random number generator vulnerability in the authenticator of the Identity Based Encryption service of FortiMail 6.4.0 through 6.4.4, and 6.2.0 through 6.2.7 may allow an unauthenticated	6.4.0 ≤6.4.4, 6.2.0 ≤6.2.9, 6.2.0 <6.2.*	Mar 24, 2025, 6:31:01 PM	Mar 24, 2025, 6:31:01 PM	http http

								attacker to infer parts of users authentication tokens and reset their credentials.				
EUVD-2018-20790	CVE-2018-9193, GSD-2018-9193,	Not available	v3.1: 7.1	0.06	FortiClientWindows, FortiClientWindows, Fortinet FortiClient for Windows	Fortinet	Mar 24, 2025, 6:30:31 PM	A researcher has disclosed several vulnerabilities against FortiClient for Windows version 6.0.5 and below, version 5.6.6, the combination of these vulnerabilities can turn into an exploit chain, which allows a user to gain system privileges on Microsoft Windows.	5.6.6, 6.0.0 ≤6.0.5, 6.0.4 and earlier	May 24, 2022, 4:46:54 PM	Mar 24, 2025, 6:30:31 PM	http http
EUVD-2025-7234	CVE-2019-16151, GHSA-c55x-8r3h-3586,	Not available	v3.1: 4.7	0.02	FortiOS, FortiOS	Fortinet	Mar 21, 2025, 4:22:17 PM	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiOS 6.4.1 and below, 6.2.9 and below may allow a remote unauthenticated attacker to either redirect users to malicious websites via a crafted "Host" header or to execute JavaScript code in the victim's browser context. This happens when the FortiGate has web filtering and category override enabled/configured.	6.4.0 ≤6.4.1, 6.2.0 ≤6.2.9	Mar 21, 2025, 4:02:01 PM	Mar 21, 2025, 4:22:17 PM	http http
EUVD-2025-3725	CVE-2025-24472,	Not available	v3.1: 8.1	8.63	FortiProxy, FortiOS, FortiProxy	Fortinet	Mar 19, 2025, 9:30:44 PM	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS 7.0.0 through 7.0.16 and FortiProxy 7.2.0 through 7.2.12, 7.0.0 through 7.0.19 may allow a remote attacker to gain super-admin privileges via crafted CSF proxy requests.	7.2.0 ≤7.2.12, 7.0.0 ≤7.0.16, 7.0.0 ≤7.0.19	Feb 11, 2025, 6:31:36 PM	Mar 19, 2025, 9:30:44 PM	http http
EUVD-2024-42864	CVE-2024-47571,	Not available	v3.1: 7.9	0.3	FortiManager, FortiManager, FortiManager, FortiManager	Fortinet	Mar 19, 2025, 6:30:48 PM	An operation on a resource after expiration or release in Fortinet FortiManager 6.4.12 through 7.4.0 allows an attacker to gain improper access to FortiGate via valid credentials.	7.0.7 ≤7.0.8, 7.2.3, 7.4.0, 6.4.12	Jan 14, 2025, 3:30:54 PM	Mar 19, 2025, 6:30:48 PM	http http
EUVD-2023-51650	CVE-2023-47539, GSD-2023-47539,	Not available	v3.1: 9.0	0.08	FortiMail	Fortinet	Mar 19, 2025, 3:55:48 AM	An improper access control vulnerability in FortiMail version 7.4.0 configured with RADIUS authentication and remote_wildcard enabled may allow a remote unauthenticated attacker to bypass admin login via a crafted HTTP request.	7.4.0	Mar 18, 2025, 1:56:56 PM	Mar 19, 2025, 3:55:48 AM	http
EUVD-2024-19374	CVE-2024-21760, GSD-2024-21760,	Not available	v3.1: 7.7	0.03	FortiSOAR, FortiSOAR, FortiSOAR, FortiSOAR, FortiSOAR, FortiSOAR	Fortinet	Mar 18, 2025, 2:15:03 PM	An improper control of generation of code ('Code Injection') vulnerability [CWE-94] in FortiSOAR Connector FortiSOAR 7.4 all versions, 7.3 all versions, 7.2 all versions, 7.0 all versions, 6.4 all versions may allow an authenticated attacker to execute arbitrary code on the	7.3.0 ≤7.3.3, 7.2.0 ≤7.2.2, 7.4.0 ≤7.4.5, 7.0.0 ≤7.0.3, 6.4.0 ≤6.4.1, 6.4.3 ≤6.4.4	Mar 18, 2025, 1:56:44 PM	Mar 18, 2025, 2:15:03 PM	http

								host via a playbook code snippet.				
EUVD-2021-9282	CVE-2021-22126, GSD-2021-22126,	Not available	v3.1: 6.5	0.02	FortiWLC, FortiWLC, FortiWLC, FortiWLC, FortiWLC	Fortinet	Mar 18, 2025, 3:55:16 AM	A use of hard-coded password vulnerability in FortiWLC version 8.5.2 and below, version 8.4.8 and below, version 8.3.3 to 8.3.2, version 8.2.7 to 8.2.6 may allow a local, authenticated attacker to connect to the managed Access Point (Meru AP and FortiAP-U) as root using the default hard-coded username and password.	8.4.0 ≤8.4.2, 8.4.4 ≤8.4.8, 8.3.2 ≤8.3.3, 8.5.0 ≤8.5.2, 8.2.6 ≤8.2.7	Mar 17, 2025, 1:05:55 PM	Mar 18, 2025, 3:55:16 AM	http http
EUVD-2025-6585	CVE-2024-54027, GHSA-qcqx-4h2x-x43j,	Not available	v3.1: 7.8	0.02	FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox	Fortinet	Mar 18, 2025, 3:55:15 AM	A Use of Hard-coded Cryptographic Key vulnerability [CWE-321] in FortiSandbox version 4.4.6 and below, version 4.2.7 and below, version 4.0.5 and below, version 3.2.4 and below, version 3.1.5 and below, version 3.0.7 to 3.0.5 may allow a privileged attacker with super-admin profile and CLI access to read sensitive data via CLI.	3.1.0 ≤3.1.5, 3.2.0 ≤3.2.4, 4.0.0 ≤4.0.5, 4.4.0 ≤4.4.6, 3.0.5 ≤3.0.7, 4.2.0 ≤4.2.7, 5.0.0	Mar 17, 2025, 1:05:31 PM	Mar 18, 2025, 3:55:15 AM	http http
EUVD-2020-30121	CVE-2020-9295, GSD-2020-9295,	Not available	v3.1: 4.7	0.02	FortiClientWindows, FortiClientWindows	Fortinet	Mar 17, 2025, 5:57:18 PM	FortiOS 6.2 running AV engine version 6.00142 and below, FortiOS 6.4 running AV engine version 6.00144 and below and FortiClient 6.2 running AV engine version 6.00137 and below may not immediately detect certain types of malformed or non-standard RAR archives, potentially containing malicious files. Based on the samples provided, FortiClient will detect the malicious files upon trying extraction by real-time scanning and FortiGate will detect the malicious archive if Virus Outbreak Prevention is enabled.	6.2.0 ≤6.2.6, 6.0.0 ≤6.0.10	Mar 17, 2025, 1:40:48 PM	Mar 17, 2025, 5:57:18 PM	http http
EUVD-2019-16255	CVE-2019-6697, GSD-2019-6697,	Not available	v3.1: 5.2	0.05	FortiOS	Fortinet	Mar 17, 2025, 5:56:56 PM	An Improper Neutralization of Input vulnerability affecting FortiGate version 6.2.0 through 6.2.1, 6.0.0 through 6.0.6 in the hostname parameter of a DHCP packet under DHCP monitor page may allow an unauthenticated attacker in the same network as the FortiGate to perform a Stored Cross Site Scripting attack (XSS) by sending a crafted DHCP packet.	6.2.0 ≤6.2.1	Mar 17, 2025, 1:40:57 PM	Mar 17, 2025, 5:56:56 PM	http http
EUVD-2025-6592	CVE-2019-15706, GHSA-c369-gmg5-w8pw,	Not available	v3.1: 4.0	0.04	FortiOS, FortiProxy, FortiProxy, FortiOS, FortiOS	Fortinet	Mar 17, 2025, 1:53:31 PM	An improper neutralization of input during web page generation in the SSL VPN portal of FortiProxy version 2.0.0, version 1.2.9 and below and FortiOS version 6.2.1 and below, version 6.0.8 and below, version 5.6.12 may	6.0.0 ≤6.0.8, 1.2.0 ≤1.2.9, 2.0.0, 6.2.0 ≤6.2.1, 5.6.12	Mar 17, 2025, 1:05:08 PM	Mar 17, 2025, 1:53:31 PM	http http

								allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS).				
EUVD-2021-12908	CVE-2021-26087, GSD-2021-26087,	Not available	v3.1: 4.2	0.04	FortiWLC, FortiWLC, FortiWLC, FortiWLC, FortiWLC	Fortinet	Mar 17, 2025, 1:52:53 PM	An improper neutralization of input during web page generation in FortiWLC version 8.6.0, version 8.5.3 and below, version 8.4.8 and below, version 8.3.3 web interface may allow both authenticated remote attackers and non-authenticated attackers in the same network as the appliance to perform a stored cross site scripting attack (XSS) via injecting malicious payloads in different locations.	8.4.0 ≤8.4.2, 8.4.4 ≤8.4.8, 8.3.3, 8.5.0 ≤8.5.3, 8.6.0	Mar 17, 2025, 1:05:19 PM	Mar 17, 2025, 1:52:53 PM	http http
EUVD-2021-19424	CVE-2021-32584, GSD-2021-32584,	Not available	v3.1: 4.8	0.04	FortiWLC, FortiWLC, FortiWLC, FortiWLC, FortiWLC, FortiWLC, FortiWLC	Fortinet	Mar 17, 2025, 1:37:26 PM	An improper access control (CWE-284) vulnerability in FortiWLC version 8.6.0, version 8.5.3 and below, version 8.4.8 and below, version 8.3.3 and below, version 8.2.7 to 8.2.4, version 8.1.3 may allow an unauthenticated and remote attacker to access certain areas of the web management CGI functionality by just specifying the correct URL. The vulnerability applies only to limited CGI resources and might allow the unauthorized party to access configuration details.	8.4.4 ≤8.4.8, 8.5.0 ≤8.5.3, 8.4.0 ≤8.4.2, 8.6.0, 8.3.0 ≤8.3.3, 8.1.3, 8.2.4 ≤8.2.7	Mar 17, 2025, 1:05:44 PM	Mar 17, 2025, 1:37:26 PM	http http
EUVD-2025-6589	CVE-2019-17659, GHSA-8f4x-4qgh-w73f,	Not available	v3.1: 3.6	0.1	FortiSIEM	Fortinet	Mar 17, 2025, 1:35:08 PM	A use of hard-coded cryptographic key vulnerability in FortiSIEM version 5.2.6 may allow a remote unauthenticated attacker to obtain SSH access to the supervisor as the restricted user "tunneluser" by leveraging knowledge of the private key from another installation or a firmware image.	5.2.6	Mar 17, 2025, 1:06:07 PM	Mar 17, 2025, 1:35:08 PM	http http
EUVD-2020-21392	CVE-2020-29010, GSD-2020-29010,	Not available	v3.1: 4.9	0.03	FortiOS, FortiOS	Fortinet	Mar 17, 2025, 1:32:38 PM	An exposure of sensitive information to an unauthorized actor vulnerability in FortiOS version 6.2.4 and below, version 6.0.10 and belowmay allow remote authenticated actors to read the SSL VPN events log entries of users in other VDOMs by executing "get vpn ssl monitor" from the CLI. The sensitive data includes usernames, user groups, and IP address.	6.2.1 ≤6.2.4, 6.0.0 ≤6.0.10	Mar 17, 2025, 1:06:16 PM	Mar 17, 2025, 1:32:38 PM	http http
EUVD-2024-54079	CVE-2024-55594,	Not available	v3.1: 5.5	0.07	FortiWeb, FortiWeb, FortiWeb	Fortinet	Mar 14, 2025, 4:25:33 PM	An improper handling of syntactically invalid structure in Fortinet FortiWeb at least vesrions 7.4.0 through 7.4.6 and 7.2.0 through 7.2.10 and 7.0.0 through 7.0.10 allows	7.4.0 ≤7.4.6, 7.2.0 ≤7.2.10, 7.0.0 ≤7.0.10	Mar 14, 2025, 4:25:33 PM	Mar 14, 2025, 4:25:33 PM	http

								attacker to execute unauthorized code or commands via HTTP/S crafted requests.				
EUVD-2023-52818	CVE-2023-48785, GSD-2023-48785,	Not available	v3.1: 4.4	100.0	FortiNAC-F	Fortinet	Mar 14, 2025, 3:46:57 PM	An improper certificate validation vulnerability [CWE-295] in FortiNAC-F version 7.2.4 and below may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the HTTPS communication channel between the FortiOS device, an inventory, and FortiNAC-F.	7.2.0 ≤7.2.4	Mar 14, 2025, 3:46:57 PM	Mar 14, 2025, 3:46:57 PM	http
EUVD-2023-37463	CVE-2023-33300, GSD-2023-33300,	Not available	v3.1: 4.8	7.78	FortiNAC, FortiNAC	Fortinet	Mar 14, 2025, 3:46:48 PM	A improper neutralization of special elements used in a command ('command injection') in Fortinet FortiNAC 7.2.1 and earlier, 9.4.3 and earlier allows attacker a limited, unauthorized file access via specifically crafted request in inter-server communication port.	9.4.0 ≤9.4.3, 7.2.0 ≤7.2.1	Mar 14, 2025, 3:46:48 PM	Mar 14, 2025, 3:46:48 PM	http
EUVD-2023-49880	CVE-2023-45588, GSD-2023-45588,	Not available	v3.1: 7.8	100.0	FortiClientMac, FortiClientMac	Fortinet	Mar 14, 2025, 3:46:35 PM	An external control of file name or path vulnerability [CWE-73] in FortiClientMac version 7.2.3 and below, version 7.0.10 and below installer may allow a local attacker to execute arbitrary code or commands via writing a malicious configuration file in /tmp before starting the installation process.	7.0.6 ≤7.0.10, 7.2.0 ≤7.2.3	Mar 14, 2025, 3:46:35 PM	Mar 14, 2025, 3:46:35 PM	http
EUVD-2024-54082	CVE-2024-40585,	Not available	v3.1: 5.9	0.02	FortiManager, FortiManager, FortiAnalyzer, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiAnalyzer, FortiManager	Fortinet	Mar 14, 2025, 3:45:46 PM	An insertion of sensitive information into log file vulnerabilities [CWE-532] in FortiManager version 7.4.0, version 7.2.3 and below, version 7.0.8 and below, version 6.4.12 and below, version 6.2.11 and below and FortiAnalyzer version 7.4.0, version 7.2.3 and below, version 7.0.8 and below, version 6.4.12 and below, version 6.2.11 and below eventlog may allow any low privileged user with access to event log section to retrieve certificate private key and encrypted password logged as system log.	7.4.0, 7.2.0 ≤7.2.3, 7.0.0 ≤7.0.8, 6.4.0 ≤6.4.12, 6.4.0 ≤6.4.12, 6.2.0 ≤6.2.11, 7.0.0 ≤7.0.8, 7.2.0 ≤7.2.3, 7.4.0, 6.2.0 ≤6.2.11	Mar 14, 2025, 3:45:46 PM	Mar 14, 2025, 3:45:46 PM	http
EUVD-2022-33472	CVE-2022-29059, GSD-2022-29059,	Not available	v3.1: 2.6	0.06	FortiWeb, FortiWeb, FortiWeb, FortiWeb	Fortinet	Mar 14, 2025, 3:45:33 PM	An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability [CWE-89] in FortiWeb version 7.0.1 and below, 6.4.2 and below, 6.3.20 and below, 6.2.7 and below may allow a privileged attacker to execute SQL commands over the log database via specifically crafted strings parameters.	6.4.0 ≤6.4.3, 6.3.0 ≤6.3.23, 7.0.0 ≤7.0.1, 6.2.3 ≤6.2.8	Mar 14, 2025, 3:45:33 PM	Mar 14, 2025, 3:45:33 PM	http

EUVD-2024-54073	CVE-2024-40590,	Not available	v3.1: 4.4	0.01	FortiPortal, FortiPortal, FortiPortal, FortiPortal	Fortinet	Mar 14, 2025, 3:32:04 PM	An improper certificate validation vulnerability [CWE-295] in FortiPortal version 7.4.0, version 7.2.4 and below, version 7.0.8 and below, version 6.0.15 and below when connecting to a FortiManager device, a FortiAnalyzer device, or an SMTP server may allow an unauthenticated attacker in a Man-in-the-Middle position to intercept on and tamper with the encrypted communication channel established between the FortiPortal and those endpoints.	7.4.0, 7.0.0 ≤7.0.8, 7.2.0 ≤7.2.4, 6.0.0 ≤6.0.15	Mar 14, 2025, 3:32:04 PM	Mar 14, 2025, 3:32:04 PM	http http
EUVD-2024-54072	CVE-2024-46662,	Not available	v3.1: 8.3	0.12	FortiManager	Fortinet	Mar 14, 2025, 3:32:04 PM	A improper neutralization of special elements used in a command ('command injection') in Fortinet FortiManager versions 7.4.1 through 7.4.3, FortiManager Cloud versions 7.4.1 through 7.4.3 allows attacker to escalation of privilege via specifically crafted packets	7.4.1 ≤7.4.3	Mar 14, 2025, 3:32:04 PM	Mar 14, 2025, 3:32:04 PM	http http
EUVD-2024-54071	CVE-2024-47573,	Not available	v3.1: 6.0	0.02	FortiNDR, FortiNDR, FortiNDR, FortiNDR	Fortinet	Mar 14, 2025, 3:32:04 PM	An improper validation of integrity check value vulnerability [CWE-354] in FortiNDR version 7.4.2 and below, version 7.2.1 and below, version 7.1.1 and below, version 7.0.6 and below may allow an authenticated attacker with at least Read/Write permission on system maintenance to install a corrupted firmware image.	7.2.0 ≤7.2.1, 7.0.0 ≤7.0.6, 7.4.0 ≤7.4.2, 7.1.0 ≤7.1.1	Mar 14, 2025, 3:32:04 PM	Mar 14, 2025, 3:32:04 PM	http http
EUVD-2024-23302	CVE-2024-26006, GSD-2024-26006,	Not available	v3.1: 6.9	0.05	FortiOS, FortiProxy, FortiOS, FortiProxy, FortiOS, FortiOS, FortiProxy	Fortinet	Mar 14, 2025, 1:09:27 PM	An improper neutralization of input during web page Generation vulnerability [CWE-79] in FortiOS version 7.4.3 and below, version 7.2.7 and below, version 7.0.13 and below and FortiProxy version 7.4.3 and below, version 7.2.9 and below, version 7.0.16 and below web SSL VPN UI may allow a remote unauthenticated attacker to perform a Cross-Site Scripting attack via a malicious samba server.	7.4.0 ≤7.4.3, 7.2.0 ≤7.2.9, 6.4.0 ≤6.4.15, 7.0.0 ≤7.0.16, 7.0.0 ≤7.0.13, 7.2.0 ≤7.2.7, 7.4.0 ≤7.4.3	Mar 14, 2025, 9:24:56 AM	Mar 14, 2025, 1:09:27 PM	http http
EUVD-2024-54213	CVE-2024-46663,	Not available	v3.1: 6.5	0.02	FortiMail, FortiMail, FortiMail, FortiMail, FortiMail	Fortinet	Mar 12, 2025, 4:00:58 AM	A stack-buffer overflow vulnerability [CWE-121] in Fortinet FortiMail CLI version 7.6.0 through 7.6.1 and before 7.4.3 allows a privileged attacker to execute arbitrary code or commands via specifically crafted CLI commands.	7.6.0 ≤7.6.1, 6.4.0 ≤6.4.8, 7.4.0 ≤7.4.3, 7.0.0 ≤7.0.8, 7.2.0 ≤7.2.7	Mar 11, 2025, 2:54:31 PM	Mar 12, 2025, 4:00:58 AM	http
EUVD-2024-54238	CVE-2024-52961,	Not available	v3.1: 8.6	0.07	FortiSandbox, FortiSandbox, FortiSandbox,	Fortinet	Mar 12, 2025, 4:00:57 AM	An improper neutralization of special elements	3.0.0 ≤3.0.7, 3.1.0	Mar 11, 2025, 2:54:30 PM	Mar 12, 2025, 4:00:57 AM	http

					FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox			used in an OS Command vulnerability [CWE-78] in Fortinet FortiSandbox version 5.0.0, 4.4.0 through 4.4.7, 4.2.0 through 4.2.7 and before 4.0.5 allows an authenticated attacker with at least read-only permission to execute unauthorized commands via crafted requests.	≤3.1.5, 5.0.0, 4.2.0 ≤4.2.7, 3.2.0 ≤3.2.4, 4.0.0 ≤4.0.5, 4.4.0 ≤4.4.6			
EUVD-2024-54212	CVE-2024-45328,	Not available	v3.1: 7.1	0.01	FortiSandbox	Fortinet	Mar 12, 2025, 4:00:56 AM	An incorrect authorization vulnerability [CWE-863] in FortiSandbox 4.4.0 through 4.4.6 may allow a low priviledged administrator to execute elevated CLI commands via the GUI console menu.	4.4.0 ≤4.4.6	Mar 11, 2025, 2:54:28 PM	Mar 12, 2025, 4:00:56 AM	http
EUVD-2024-54211	CVE-2024-45324,	Not available	v3.1: 7.0	0.17	FortiProxy, FortiOS, FortiPAM, FortiWeb, FortiPAM, FortiPAM, FortiPAM, FortiSRA, FortiWeb, FortiOS, FortiProxy, FortiWeb, FortiPAM, FortiOS, FortiProxy, FortiOS, FortiProxy, FortiWeb, FortiOS	Fortinet	Mar 12, 2025, 4:00:50 AM	A use of externally-controlled format string vulnerability [CWE-134] in FortiOS version 7.4.0 through 7.4.4, version 7.2.0 through 7.2.9, version 7.0.0 through 7.0.15 and before 6.4.15, FortiProxy version 7.4.0 through 7.4.6, version 7.2.0 through 7.2.12 and before 7.0.19, FortiPAM version 1.4.0 through 1.4.2 and before 1.3.1, FortiSRA version 1.4.0 through 1.4.2 and before 1.3.1 and FortiWeb version 7.4.0 through 7.4.5, version 7.2.0 through 7.2.10 and before 7.0.10 allows a privileged attacker to execute unauthorized code or commands via specially crafted HTTP or HTTPS commands.	7.2.0 ≤7.2.12, 7.0.0 ≤7.0.15, 1.4.0 ≤1.4.2, 7.2.0 ≤7.2.10, 1.2.0, 1.0.0 ≤1.0.3, 1.1.0 ≤1.1.2, 1.4.0 ≤1.4.2, 7.6.0, 7.2.0 ≤7.2.9, 7.0.0 ≤7.0.19, 7.0.0 ≤7.0.10, 1.3.0 ≤1.3.1, 7.4.0 ≤7.4.4, 7.4.0 ≤7.4.6, 6.2.0 ≤6.2.16, 7.6.0, 7.4.0 ≤7.4.5, 6.4.0 ≤6.4.15	Mar 11, 2025, 2:54:33 PM	Mar 12, 2025, 4:00:50 AM	http
EUVD-2023-45277	CVE-2023-40723, GSD-2023-40723,	Not available	v3.1: 7.7	0.06	FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM	Fortinet	Mar 12, 2025, 4:00:49 AM	An exposure of sensitive information to an unauthorized actor in Fortinet FortiSIEM version 6.7.0 through 6.7.4 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.1 and 6.4.0 through 6.4.2 and 6.3.0 through 6.3.3 and 6.2.0 through 6.2.1 and 6.1.0 through 6.1.2 and 5.4.0 and 5.3.0 through 5.3.3 and 5.2.5 through 5.2.8 and 5.2.1 through 5.2.2 and 5.1.0 through 5.1.3 allows attacker to execute unauthorized code or commands via api request.	5.3.0 ≤5.3.3, 6.3.0 ≤6.3.3, 5.2.1 ≤5.2.2, 5.2.5 ≤5.2.8, 6.5.0 ≤6.5.1, 6.6.0 ≤6.6.3, 6.4.0 ≤6.4.2, 6.7.0 ≤6.7.4, 5.4.0, 6.2.0 ≤6.2.1, 5.1.0 ≤5.1.3, 6.1.0 ≤6.1.2	Mar 11, 2025, 2:54:28 PM	Mar 12, 2025, 4:00:49 AM	http
EUVD-2023-41786	CVE-2023-37933, GSD-2023-37933,	Not available	v3.1: 8.6	0.09	FortiADC, FortiADC, FortiADC, FortiADC, FortiADC, FortiADC, FortiADC, FortiADC, FortiADC	Fortinet	Mar 12, 2025, 4:00:48 AM	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiADC GUI version 7.4.0, 7.2.0 through 7.2.1 and before 7.1.3 allows an authenticated attacker to perform an XSS attack via	7.2.0 ≤7.2.1, 7.4.0, 5.3.0 ≤5.3.7, 7.0.0 ≤7.0.5, 6.0.0 ≤6.0.4, 5.4.0 ≤5.4.5, 6.1.0 ≤6.1.6,	Mar 11, 2025, 2:54:35 PM	Mar 12, 2025, 4:00:48 AM	http

								crafted HTTP or HTTPs requests.	6.2.0 ≤6.2.6, 7.1.0 ≤7.1.3			
EUVD-2024-54249	CVE-2024-54018,	Not available	v3.1: 6.8	0.08	FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox	Fortinet	Mar 12, 2025, 4:00:46 AM	Multiple improper neutralization of special elements used in an OS Command vulnerabilities [CWE-78] in FortiSandbox before 4.4.5 allows a privileged attacker to execute unauthorized commands via crafted requests.	4.4.0 ≤4.4.4, 4.2.0 ≤4.2.6, 4.0.0 ≤4.0.6, 3.2.0 ≤3.2.4	Mar 11, 2025, 2:54:37 PM	Mar 12, 2025, 4:00:46 AM	http
EUVD-2024-29944	CVE-2024-32123, GSD-2024-32123,	Not available	v3.1: 6.5	0.05	FortiManager, FortiManager, FortiAnalyzer, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager, FortiManager, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager, FortiManager, FortiManager, FortiManager, FortiManager	Fortinet	Mar 12, 2025, 4:00:45 AM	Multiple improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiManager, FortiAnalyzer versions 7.4.0 through 7.4.2 7.2.0 through 7.2.5 and 7.0.0 through 7.0.12 and 6.4.0 through 6.4.14 and 6.2.0 through 6.2.12 and 6.0.0 through 6.0.12 and 5.6.0 through 5.6.11 and 5.4.0 through 5.4.7 and 5.2.0 through 5.2.10 and 5.0.0 through 5.0.12 and 4.3.4 through 4.3.8 allows attacker to execute unauthorized code or commands via crafted CLI requests.	4.3.4 ≤4.3.8, 5.2.0 ≤5.2.10, 7.4.0 ≤7.4.2, 7.2.0 ≤7.2.5, 5.0.0 ≤5.0.12, 7.0.0 ≤7.0.13, 7.4.0 ≤7.4.2, 6.4.0 ≤6.4.15, 6.2.0 ≤6.2.13, 6.2.0 ≤6.2.13, 6.4.0 ≤6.4.15, 7.0.0 ≤7.0.13, 6.0.0 ≤6.0.12, 5.4.0 ≤5.4.7, 5.6.0 ≤5.6.11, 7.2.0 ≤7.2.5	Mar 11, 2025, 2:54:38 PM	Mar 12, 2025, 4:00:45 AM	http
EUVD-2023-47214	CVE-2023-42784, GSD-2023-42784,	Not available	v3.1: 5.5	0.07	FortiWeb, FortiWeb, FortiWeb	Fortinet	Mar 11, 2025, 4:10:57 PM	An improper handling of syntactically invalid structure in Fortinet FortiWeb at least verions 7.4.0 through 7.4.6 and 7.2.0 through 7.2.10 and 7.0.0 through 7.0.10 allows attacker to execute unauthorized code or commands via HTTP/S crafted requests.	7.2.0 ≤7.2.10, 7.0.0 ≤7.0.10, 7.4.0 ≤7.4.7	Mar 11, 2025, 2:54:28 PM	Mar 11, 2025, 4:10:57 PM	http
EUVD-2024-54266	CVE-2024-55592,	Not available	v3.1: 3.6	0.02	FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM	Fortinet	Mar 11, 2025, 4:07:03 PM	An incorrect authorization vulnerability [CWE-863] in FortiSIEM 7.2 all versions, 7.1 all versions, 7.0 all versions, 6.7 all versions, 6.6 all versions, 6.5 all versions, 6.4 all versions, 6.3 all versions, 6.2 all versions, 6.1 all versions, 5.4 all versions, 5.3 all versions, may allow an authenticated attacker to perform unauthorized operations on incidents via crafted HTTP requests.	7.0.0 ≤7.0.3, 6.3.0 ≤6.3.3, 6.6.0 ≤6.6.5, 6.1.0 ≤6.1.2, 7.2.0 ≤7.2.5, 6.7.0 ≤6.7.9, 5.4.0, 6.4.0 ≤6.4.4, 5.3.0 ≤5.3.3, 7.1.0 ≤7.1.7, 6.2.0 ≤6.2.1, 6.5.0 ≤6.5.3	Mar 11, 2025, 2:54:29 PM	Mar 11, 2025, 4:07:03 PM	http
EUVD-2024-54267	CVE-2024-55597,	Not available	v3.1: 5.2	0.08	FortiWeb, FortiWeb, FortiWeb, FortiWeb	Fortinet	Mar 11, 2025, 4:06:25 PM	A improper limitation of a pathname to a restricted directory ('path traversal') in Fortinet FortiWeb versions 7.0.0 through 7.6.0 allows attacker to execute unauthorized code or commands via crafted requests.	7.2.0 ≤7.2.10, 7.4.0 ≤7.4.5, 7.0.0 ≤7.0.10, 7.6.0	Mar 11, 2025, 2:54:26 PM	Mar 11, 2025, 4:06:25 PM	http

EUVD-2023-52823	CVE-2023-48790, GSD-2023-48790,	Not available	v3.1: 7.1	0.09	FortiNDR, FortiNDR, FortiNDR, FortiNDR, FortiNDR	Fortinet	Mar 11, 2025, 4:05:58 PM	A cross site request forgery vulnerability [CWE-352] in Fortinet FortiNDR version 7.4.0, 7.2.0 through 7.2.1 and 7.1.0 through 7.1.1 and before 7.0.5 may allow a remote unauthenticated attacker to execute unauthorized actions via crafted HTTP GET requests.	7.4.0, 7.2.0 ≤7.2.1, 7.0.0 ≤7.0.5, 7.1.0 ≤7.1.1, 1.5.0 ≤1.5.3	Mar 11, 2025, 2:54:31 PM	Mar 11, 2025, 4:05:58 PM	http
EUVD-2024-54265	CVE-2024-55590,	Not available	v3.1: 8.6	0.24	FortiIsolator	Fortinet	Mar 11, 2025, 4:05:38 PM	Multiple improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiIsolator version 2.4.0 through 2.4.5 allows an authenticated attacker with at least read-only admin permission and CLI access to execute unauthorized code via specifically crafted CLI commands.	2.4.0 ≤2.4.5	Mar 11, 2025, 2:54:34 PM	Mar 11, 2025, 4:05:38 PM	http
EUVD-2024-54237	CVE-2024-52960,	Not available	v3.1: 4.2	0.03	FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox	Fortinet	Mar 11, 2025, 4:05:31 PM	A client-side enforcement of server-side security vulnerability [CWE-602] in Fortinet FortiSandbox version 5.0.0, 4.4.0 through 4.4.6 and before 4.2.7 allows an authenticated attacker with at least read-only permission to execute unauthorized commands via crafted requests.	5.0.0, 4.0.0 ≤4.0.6, 3.2.0 ≤3.2.4, 4.2.0 ≤4.2.7, 3.0.0 ≤3.0.7, 4.4.0 ≤4.4.6, 3.1.0 ≤3.1.5	Mar 11, 2025, 2:54:35 PM	Mar 11, 2025, 4:05:31 PM	http
EUVD-2024-54250	CVE-2024-54026,	Not available	v3.1: 4.1	0.04	FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox	Fortinet	Mar 11, 2025, 4:05:02 PM	An improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiSandbox Cloud version 23.4, FortiSandbox at least 4.4.0 through 4.4.6 and 4.2.0 through 4.2.7 and 4.0.0 through 4.0.5 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.7 allows attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	4.4.0 ≤4.4.6, 3.0.0 ≤3.0.7, 4.2.0 ≤4.2.8, 3.2.0 ≤3.2.4, 3.1.0 ≤3.1.5, 4.0.0 ≤4.0.6	Mar 11, 2025, 2:54:38 PM	Mar 11, 2025, 4:05:02 PM	http
EUVD-2024-31239	CVE-2024-33501, GSD-2024-33501,	Not available	v3.1: 4.0	0.02	FortiManager, FortiManager, FortiManager, FortiManager, FortiManager, FortiManager	Fortinet	Mar 11, 2025, 4:04:54 PM	Two improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerability [CWE-89] in Fortinet FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5, FortiManager version 7.4.0 through 7.4.2 and before 7.2.5 and FortiAnalyzer-BigData version 7.4.0 and before 7.2.7 allows a privileged attacker to execute unauthorized code or commands via specifically crafted CLI requests.	7.2.0 ≤7.2.5, 6.4.4 ≤6.4.15, 6.0.10 ≤6.0.12, 6.2.8 ≤6.2.13, 7.4.0 ≤7.4.2, 7.0.0 ≤7.0.13	Mar 11, 2025, 2:54:41 PM	Mar 11, 2025, 4:04:54 PM	http
EUVD-2023-51653	CVE-2023-	Not available	v3.1: 6.3	0.07	FortiManager, FortiManager,	Fortinet	Feb 26, 2025,	A improper neutralization of	7.0.0 ≤7.0.10,	Apr 9, 2024, 2:24:24 PM	Feb 26, 2025,	http

	47542, GSD-2023-47542,				FortiManager		6:40:53 PM	special elements used in a template engine [CWE-1336] in FortiManager versions 7.4.1 and below, versions 7.2.4 and below, and 7.0.10 and below allows attacker to execute unauthorized code or commands via specially crafted templates.	7.4.0 ≤7.4.1, 7.2.0 ≤7.2.4		6:40:53 PM	
EUVD-2024-42217	CVE-2024-46666,	Not available	v3.1: 4.8	0.08	FortiOS, FortiOS, FortiOS, FortiOS, FortiOS	Fortinet	Feb 18, 2025, 9:39:30 PM	An allocation of resources without limits or throttling [CWE-770] vulnerability in FortiOS versions 7.6.0, versions 7.4.4 through 7.4.0, 7.2 all versions, 7.0 all versions, 6.4 all versions may allow a remote unauthenticated attacker to prevent access to the GUI via specially crafted requests directed at specific endpoints.	7.2.0 ≤7.2.10, 7.0.0 ≤7.0.16, 7.6.0, 7.4.0 ≤7.4.4, 6.4.0 ≤6.4.15	Jan 14, 2025, 2:09:56 PM	Feb 18, 2025, 9:39:30 PM	http
EUVD-2024-19372	CVE-2024-21758, GSD-2024-21758,	Not available	v3.1: 6.1	0.02	FortiWeb, FortiWeb	Fortinet	Feb 18, 2025, 9:38:54 PM	A stack-based buffer overflow in Fortinet FortiWeb versions 7.2.0 through 7.2.7, and 7.4.0 through 7.4.1 may allow a privileged user to execute arbitrary code via specially crafted CLI commands, provided the user is able to evade FortiWeb stack protections.	7.2.0 ≤7.2.7, 7.4.0 ≤7.4.1	Jan 14, 2025, 2:09:56 PM	Feb 18, 2025, 9:38:54 PM	http
EUVD-2024-36358	CVE-2024-36504,	Not available	v3.1: 6.2	0.08	FortiOS, FortiOS, FortiOS, FortiOS	Fortinet	Feb 18, 2025, 9:38:19 PM	An out-of-bounds read vulnerability [CWE-125] in FortiOS SSLVPN web portal versions 7.4.0 through 7.4.4, versions 7.2.0 through 7.2.8, 7.0 all verisons, and 6.4 all versions may allow an authenticated attacker to perform a denial of service on the SSLVPN web portal via a specially crafted URL.	7.2.0 ≤7.2.8, 6.4.0 ≤6.4.15, 7.4.0 ≤7.4.4, 7.0.0 ≤7.0.16	Jan 14, 2025, 2:09:58 PM	Feb 18, 2025, 9:38:19 PM	http
EUVD-2024-42207	CVE-2024-46667,	Not available	v3.1: 6.9	0.06	FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM, FortiSIEM	Fortinet	Feb 18, 2025, 9:37:18 PM	A allocation of resources without limits or throttling in Fortinet FortiSIEM 5.3 all versions, 5.4 all versions, 6.x all versions, 7.0 all versions, and 7.1.0 through 7.1.5 may allow an attacker to deny valid TLS traffic via consuming all allotted connections.	6.1.0 ≤6.1.2, 7.1.0 ≤7.1.5, 6.7.0 ≤6.7.9, 5.4.0, 5.3.0 ≤5.3.3, 7.0.0 ≤7.0.3, 6.4.0 ≤6.4.4, 6.2.0 ≤6.2.1, 6.3.0 ≤6.3.3, 6.6.0 ≤6.6.5, 6.5.0 ≤6.5.3	Jan 14, 2025, 2:09:58 PM	Feb 18, 2025, 9:37:18 PM	http
EUVD-2024-42865	CVE-2024-47572,	Not available	v3.1: 8.3	0.06	FortiSOAR, FortiSOAR, FortiSOAR	Fortinet	Feb 18, 2025, 9:36:45 PM	An improper neutralization of formula elements in a csv file in Fortinet FortiSOAR 7.2.1 through 7.4.1 allows attacker to execute unauthorized code or commands via manipulating csv file	7.4.0 ≤7.4.1, 7.3.0 ≤7.3.2, 7.2.1 ≤7.2.2	Jan 14, 2025, 2:09:59 PM	Feb 18, 2025, 9:36:45 PM	http
EUVD-2023-41784	CVE-2023-37931,	Not available	v3.1: 8.6	0.13	FortiVoice, FortiVoice, FortiVoice	Fortinet	Feb 18, 2025, 9:35:20 PM	An improper neutralization of special elements	7.0.0 ≤7.0.1, 6.4.0	Jan 14, 2025, 2:10:00 PM	Feb 18, 2025, 9:35:20 PM	http

	GSD-2023-37931,							used in an sql command ('sql injection') vulnerability [CWE-88] in FortiVoice Entreprise version 7.0.0 through 7.0.1 and before 6.4.8 allows an authenticated attacker to perform a blind sql injection attack via sending crafted HTTP or HTTPS requests	≤6.4.8, 6.0.0 ≤6.0.12			
EUVD-2024-20631	CVE-2024-23106, GSD-2024-23106,	Not available	v3.1: 7.7	0.08	FortiClientEMS, FortiClientEMS, FortiClientEMS, FortiClientEMS, FortiClientEMS, FortiClientEMS	Fortinet	Feb 18, 2025, 9:34:28 PM	An improper restriction of excessive authentication attempts [CWE-307] in FortiClientEMS version 7.2.0 through 7.2.4 and before 7.0.10 allows an unauthenticated attacker to try a brute force attack against the FortiClientEMS console via crafted HTTP or HTTPS requests.	6.4.0 ≤6.4.4, 7.0.0 ≤7.0.10, 6.4.7 ≤6.4.9, 6.2.0 ≤6.2.4, 6.2.6 ≤6.2.9, 7.2.0 ≤7.2.3	Jan 14, 2025, 2:10:00 PM	Feb 18, 2025, 9:34:28 PM	http
EUVD-2024-29936	CVE-2024-32115, GSD-2024-32115,	Not available	v3.1: 5.2	0.24	FortiManager, FortiManager, FortiManager	Fortinet	Feb 18, 2025, 9:33:30 PM	A relative path traversal vulnerability [CWE-23] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5 allows a privileged attacker to delete files from the underlying filesystem via crafted HTTP or HTTPs requests.	7.0.0 ≤7.0.13, 7.4.0 ≤7.4.2, 7.2.0 ≤7.2.5	Jan 14, 2025, 2:10:01 PM	Feb 18, 2025, 9:33:30 PM	http
EUVD-2025-4981	CVE-2024-40591, GHSA-hmpg-p67j-959p,	Not available	v3.1: 8.0	0.05	FortiOS, FortiOS, FortiOS, FortiOS, FortiOS	Fortinet	Feb 14, 2025, 4:55:21 AM	An incorrect privilege assignment vulnerability [CWE-266] in Fortinet FortiOS version 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.9 and before 7.0.15 allows an authenticated admin whose access profile has the Security Fabric permission to escalate their privileges to super-admin by connecting the targetted FortiGate to a malicious upstream FortiGate they control.	7.4.0 ≤7.4.4, 6.4.0 ≤6.4.15, 7.6.0, 7.2.0 ≤7.2.9, 7.0.0 ≤7.0.15	Feb 11, 2025, 4:09:02 PM	Feb 14, 2025, 4:55:21 AM	http http
EUVD-2025-4982	CVE-2024-35279, GHSA-8ccx-r52j-39f8,	Not available	v3.1: 7.7	0.13	FortiOS, FortiOS	Fortinet	Feb 14, 2025, 4:55:19 AM	A stack-based buffer overflow [CWE-121] vulnerability in Fortinet FortiOS version 7.2.4 through 7.2.8 and version 7.4.0 through 7.4.4 allows a remote unauthenticated attacker to execute arbitrary code or commands via crafted UDP packets through the CAPWAP control, provided the attacker were able to evade FortiOS stack protections and provided the fabric service is running on the exposed interface.	7.4.0 ≤7.4.4, 7.2.4 ≤7.2.8	Feb 11, 2025, 4:09:02 PM	Feb 14, 2025, 4:55:19 AM	http http
EUVD-2025-4973	CVE-2024-50569, GHSA-x7j3-3mr3-jq5q,	Not available	v3.1: 6.3	0.26	FortiWeb, FortiWeb, FortiWeb, FortiWeb	Fortinet	Feb 14, 2025, 4:55:18 AM	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb 7.0.0 through 7.6.0 allows attacker to execute unauthorized code or	7.2.0 ≤7.2.10, 7.4.0 ≤7.4.5, 7.6.0, 7.0.0 ≤7.0.10	Feb 11, 2025, 4:09:00 PM	Feb 14, 2025, 4:55:18 AM	http http

								commands via crafted input.				
EUVD-2025-4978	CVE-2024-50567, GHSA-g5rj-645r-67rh,	Not available	v3.1: 6.8	0.26	FortiWeb, FortiWeb	Fortinet	Feb 14, 2025, 4:55:16 AM	An improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb 7.4.0 through 7.6.0 allows attacker to execute unauthorized code or commands via crafted input.	7.4.0 ≤7.4.5, 7.6.0	Feb 11, 2025, 4:09:04 PM	Feb 14, 2025, 4:55:16 AM	http http
EUVD-2024-24974	CVE-2024-27781, GSD-2024-27781,	Not available	v3.1: 6.9	0.13	FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox, FortiSandbox	Fortinet	Feb 14, 2025, 4:55:15 AM	An improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox at least versions 4.4.0 through 4.4.4 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.4 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.7 allows an authenticated attacker to execute unauthorized code or commands via crafted HTTP requests.	4.2.0 ≤4.2.6, 4.0.0 ≤4.0.4, 3.1.0 ≤3.1.5, 4.4.0 ≤4.4.4, 3.0.0 ≤3.0.7, 3.2.0 ≤3.2.4	Feb 11, 2025, 4:09:12 PM	Feb 14, 2025, 4:55:15 AM	http http
EUVD-2023-48612	CVE-2023-44253, GSD-2023-44253,	Not available	v3.1: 4.7	0.19	FortiAnalyzer, FortiManager, FortiManager, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager	Fortinet	Feb 13, 2025, 5:13:34 PM	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiManager version 7.4.0 through 7.4.1 and before 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.1 and before 7.2.5 and FortiAnalyzer-BigData before 7.2.5 allows an adom administrator to enumerate other adoms and device names via crafted HTTP or HTTPS requests.	7.2.0 ≤7.2.3, 6.2.0 ≤6.2.12, 7.2.0 ≤7.2.3, 6.2.0 ≤6.2.12, 7.4.0 ≤7.4.1, 7.0.0 ≤7.0.11, 6.4.0 ≤6.4.14, 7.0.0 ≤7.0.11, 7.4.0 ≤7.4.1, 6.4.0 ≤6.4.14	Feb 15, 2024, 1:59:24 PM	Feb 13, 2025, 5:13:34 PM	http http rese
EUVD-2023-48608	CVE-2023-44249, GSD-2023-44249,	Not available	v3.1: 4.1	0.15	FortiAnalyzer, FortiManager, FortiManager, FortiAnalyzer, FortiAnalyzer, FortiAnalyzer, FortiManager, FortiManager, FortiManager, FortiAnalyzer	Fortinet	Feb 13, 2025, 5:13:33 PM	An authorization bypass through user-controlled key [CWE-639] vulnerability in Fortinet FortiManager version 7.4.0 and before 7.2.3 and FortiAnalyzer version 7.4.0 and before 7.2.3 allows a remote attacker with low privileges to read sensitive information via crafted HTTP requests.	7.2.0 ≤7.2.3, 7.2.0 ≤7.2.3, 7.4.0, 6.4.0 ≤6.4.13, 6.2.0 ≤6.2.12, 7.4.0, 6.4.0 ≤6.4.13, 7.0.0 ≤7.0.9, 6.2.0 ≤6.2.12, 7.0.0 ≤7.0.9	Oct 10, 2023, 4:48:38 PM	Feb 13, 2025, 5:13:33 PM	http http rese
EUVD-2023-47218	CVE-2023-42788, GSD-2023-42788,	Not available	v3.1: 7.6	0.29	FortiManager, FortiManager, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager, FortiManager, FortiManager, FortiAnalyzer, FortiAnalyzer	Fortinet	Feb 13, 2025, 5:09:42 PM	An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in FortiManager & FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.8, version 6.4.0 through 6.4.12 and version 6.2.0 through 6.2.11 may allow a local attacker with low privileges to execute unauthorized code via specifically crafted arguments to	7.0.0 ≤7.0.8, 7.4.0, 6.4.0 ≤6.4.12, 7.4.0, 7.2.0 ≤7.2.3, 6.4.0 ≤6.4.12, 7.2.0 ≤7.2.3, 6.2.0 ≤6.2.11, 7.0.0 ≤7.0.8, 6.2.0 ≤6.2.11	Oct 10, 2023, 4:48:56 PM	Feb 13, 2025, 5:09:42 PM	http http rese

								a CLI command				
EUVD-2023-47217	CVE-2023-42787, GSD-2023-42787,	Not available	v3.1: 6.2	0.75	FortiManager, FortiAnalyzer, FortiAnalyzer, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager, FortiManager, FortiManager, FortiAnalyzer	Fortinet	Feb 13, 2025, 5:09:41 PM	A client-side enforcement of server-side security [CWE-602] vulnerability in Fortinet FortiManager version 7.4.0 and before 7.2.3 and FortiAnalyzer version 7.4.0 and before 7.2.3 may allow a remote attacker with low privileges to access a privileged web console via client side code execution.	7.2.0 ≤7.2.3, 6.4.0 ≤6.4.13, 6.2.0 ≤6.2.12, 7.2.0 ≤7.2.3, 7.0.0 ≤7.0.9, 7.4.0, 7.4.0, 6.2.0 ≤6.2.12, 6.4.0 ≤6.4.13, 7.0.0 ≤7.0.9	Oct 10, 2023, 4:48:46 PM	Feb 13, 2025, 5:09:41 PM	http http rese
EUVD-2022-44540	CVE-2022-41333, GSD-2022-41333,	Not available	v3.1: 6.8	8.39	FortiRecorder, FortiRecorder	Fortinet	Feb 13, 2025, 4:33:04 PM	An uncontrolled resource consumption vulnerability [CWE-400] in FortiRecorder version 6.4.3 and below, 6.0.11 and below login authentication mechanism may allow an unauthenticated attacker to make the device unavailable via crafted GET requests.	6.0.0 ≤6.0.11, 6.4.0 ≤6.4.3	Mar 7, 2023, 4:04:43 PM	Feb 13, 2025, 4:33:04 PM	http http 6.4.
EUVD-2025-4974	CVE-2024-40584, GHSA-x763-rwjp-4g28,	Not available	v3.1: 6.8	0.4	FortiManager, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiAnalyzer, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager, FortiManager	Fortinet	Feb 12, 2025, 3:53:33 PM	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiAnalyzer version 7.4.0 through 7.4.3, 7.2.0 through 7.2.5, 7.0.0 through 7.0.13, 6.4.0 through 6.4.15 and 6.2.2 through 6.2.13, Fortinet FortiManager version 7.4.0 through 7.4.3, 7.2.0 through 7.2.5, 7.0.0 through 7.0.13, 6.4.0 through 6.4.15 and 6.2.2 through 6.2.13, Fortinet FortiAnalyzer BigData version 7.4.0, 7.2.0 through 7.2.7, 7.0.1 through 7.0.6, 6.4.5 through 6.4.7 and 6.2.5, Fortinet FortiAnalyzer Cloud version 7.4.1 through 7.4.3, 7.2.1 through 7.2.5, 7.0.1 through 7.0.13 and 6.4.1 through 6.4.7 and Fortinet FortiManager Cloud version 7.4.1 through 7.4.3, 7.2.1 through 7.2.5, 7.0.1 through 7.0.13 and 6.4.1 through 6.4.7 GUI allows an authenticated privileged attacker to execute unauthorized code or commands via crafted HTTPS or HTTP requests.	7.4.0 ≤7.4.3, 7.0.0 ≤7.0.13, 7.0.0 ≤7.0.13, 6.2.2 ≤6.2.13, 7.2.0 ≤7.2.5, 6.4.0 ≤6.4.15, 7.2.0 ≤7.2.5, 7.4.0 ≤7.4.3, 6.2.2 ≤6.2.13, 6.4.0 ≤6.4.15	Feb 11, 2025, 4:09:07 PM	Feb 12, 2025, 3:53:33 PM	http http
EUVD-2025-4979	CVE-2024-36508, GHSA-7w3h-vqp8-323r,	Not available	v3.1: 5.9	0.07	FortiAnalyzer, FortiAnalyzer, FortiAnalyzer, FortiManager, FortiAnalyzer, FortiManager, FortiManager, FortiManager	Fortinet	Feb 12, 2025, 3:53:19 PM	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5 and Fortinet FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5 CLI allows an authenticated admin	7.0.0 ≤7.0.13, 7.4.0 ≤7.4.2, 7.2.0 ≤7.2.5, 7.0.0 ≤7.0.13, 6.4.0 ≤6.4.15, 7.4.0 ≤7.4.2, 6.4.0 ≤6.4.15, 7.2.0	Feb 11, 2025, 4:09:07 PM	Feb 12, 2025, 3:53:19 PM	http http

								user with diagnose privileges to delete files on the system.	≤7.2.5			
EUVD-2025-4983	CVE-2024-40586, GHSA-89gg-gc7x-gwhp,	Not available	v3.1: 6.3	0.02	FortiClientWindows, FortiClientWindows, FortiClientWindows	Fortinet	Feb 12, 2025, 3:53:08 PM	An Improper Access Control vulnerability [CWE-284] in FortiClient Windows version 7.4.0, version 7.2.6 and below, version 7.0.13 and below may allow a local user to escalate his privileges via FortiSSLVPNd service pipe.	7.4.0, 7.0.3 ≤7.0.13, 7.2.0 ≤7.2.6	Feb 11, 2025, 4:09:06 PM	Feb 12, 2025, 3:53:08 PM	http http
EUVD-2023-45275	CVE-2023-40721, GSD-2023-40721,	Not available	v3.1: 6.3	0.02	FortiPAM, FortiOS, FortiProxy, FortiProxy, FortiOS, FortiSwitchManager, FortiOS, FortiPAM, FortiProxy, FortiSwitchManager, FortiOS, FortiProxy, FortiProxy, FortiOS	Fortinet	Feb 12, 2025, 3:52:51 PM	A use of externally-controlled format string vulnerability [CWE-134] in Fortinet FortiOS version 7.4.0 through 7.4.1 and before 7.2.6, FortiProxy version 7.4.0 and before 7.2.7, FortiPAM version 1.1.2 and before 1.0.3, FortiSwitchManager version 7.2.0 through 7.2.2 and before 7.0.2 allows a privileged attacker to execute arbitrary code or commands via specially crafted requests.	1.1.0 ≤1.1.2, 7.4.0, 2.0.0 ≤2.0.14, 1.2.0 ≤1.2.13, 6.2.0 ≤6.2.16, 7.2.0 ≤7.2.2, 7.0.0 ≤7.0.13, 1.0.0 ≤1.0.3, 7.4.0, 7.0.0 ≤7.0.2, 7.2.0 ≤7.2.5, 7.0.0 ≤7.0.14, 7.2.0 ≤7.2.6, 6.4.0 ≤6.4.15	Feb 11, 2025, 4:09:06 PM	Feb 12, 2025, 3:52:51 PM	http http
EUVD-2025-4976	CVE-2024-52966, GHSA-hpjc-rrq5-mqv8,	Not available	v3.1: 2.2	0.02	FortiAnalyzer, FortiAnalyzer, FortiAnalyzer, FortiAnalyzer, FortiAnalyzer	Fortinet	Feb 12, 2025, 3:52:16 PM	An exposure of sensitive information to an unauthorized actor in Fortinet FortiAnalyzer 6.4.0 through 7.6.0 allows attacker to cause information disclosure via filter manipulation.	7.6.0, 6.4.0 ≤6.4.15, 7.4.0 ≤7.4.4, 7.2.0 ≤7.2.7, 7.0.0 ≤7.0.13	Feb 11, 2025, 4:09:01 PM	Feb 12, 2025, 3:52:16 PM	http http
EUVD-2024-24973	CVE-2024-27780, GSD-2024-27780,	Not available	v3.1: 2.2	0.03	FortiSIEM, FortiSIEM, FortiSIEM	Fortinet	Feb 12, 2025, 3:40:18 PM	Multiple Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerabilities [CWE-79] in FortiSIEM 7.1 all versions, 7.0 all versions, 6.7 all versions incident page may allow an authenticated attacker to perform a cross-site scripting attack via crafted HTTP requests.	7.1.0 ≤7.1.7, 6.7.0 ≤6.7.9, 7.0.0 ≤7.0.3	Feb 11, 2025, 4:09:12 PM	Feb 12, 2025, 3:40:18 PM	http http
EUVD-2025-3724	CVE-2025-24470,	Not available	v3.1: 8.1	0.3	FortiPortal, FortiPortal, FortiPortal	Fortinet	Feb 11, 2025, 4:43:10 PM	An Improper Resolution of Path Equivalence vulnerability [CWE-41] in FortiPortal 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.11 may allow a remote unauthenticated attacker to retrieve source code via crafted HTTP requests.	7.4.0 ≤7.4.2, 7.0.0 ≤7.0.11, 7.2.0 ≤7.2.6	Feb 11, 2025, 4:08:58 PM	Feb 11, 2025, 4:43:10 PM	http http
EUVD-2025-4977	CVE-2024-52968, GHSA-h55v-j7qg-4vf6,	Not available	v3.1: 5.8	0.05	FortiClientMac, FortiClientMac, FortiClientMac	Fortinet	Feb 11, 2025, 4:35:11 PM	An improper authentication in Fortinet FortiClientMac 7.0.11 through 7.2.4 allows attacker to gain improper access to MacOS via empty password.	7.4.0, 7.2.3 ≤7.2.4, 7.0.11 ≤7.0.12	Feb 11, 2025, 4:09:00 PM	Feb 11, 2025, 4:35:11 PM	http http
EUVD-2024-31242	CVE-2024-33504, GSD-	Not available	v3.1: 3.9	0.02	FortiManager, FortiManager, FortiManager, FortiManager,	Fortinet	Feb 11, 2025, 4:32:53 PM	A use of hard-coded cryptographic key to encrypt sensitive data vulnerability	7.4.0 ≤7.4.5, 7.2.0 ≤7.2.9,	Feb 11, 2025, 4:09:03 PM	Feb 11, 2025, 4:32:53 PM	http rese http http

	2024-33504,				FortiManager			[CWE-321] in FortiManager 7.6.0 through 7.6.1, 7.4.0 through 7.4.5, 7.2.0 through 7.2.9, 7.0 all versions, 6.4 all versions may allow an attacker with JSON API access permissions to decrypt some secrets even if the 'private-data-encryption' setting is enabled.	7.0.0 ≤7.0.13, 7.6.0 ≤7.6.1, 6.4.0 ≤6.4.15			
EUVD-2024-52819	CVE-2024-55591,	Not available	v3.1: 9.6	93.01	FortiOS, FortiProxy, FortiProxy	Fortinet	Jan 23, 2025, 4:55:42 AM	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module.	7.0.0 ≤7.0.16, 7.2.0 ≤7.2.12, 7.0.0 ≤7.0.19	Jan 14, 2025, 2:08:34 PM	Jan 23, 2025, 4:55:42 AM	http
EUVD-2022-28514	CVE-2022-23439, GSD-2022-23439,	Not available	v3.1: 4.1	0.07	FortiMail, FortiSwitch, FortiOS, FortiAuthenticator, FortiADC, FortiADC, FortiSOAR, FortiTester, FortiNDR, FortiSOAR, FortiManager, FortiManager, FortiSOAR, FortiVoice, FortiAnalyzer, FortiADC, FortiDDoS, FortiDDoS-F, FortiTester, FortiTester, FortiTester, FortiTester, FortiNDR, FortiWLC, FortiMail, FortiDDoS, FortiAuthenticator, FortiProxy, FortiRecorder, FortiOS, FortiManager, FortiRecorder, FortiProxy, FortiAnalyzer, FortiTester, FortiADC, FortiNDR, FortiDDoS, FortiADC, FortiAnalyzer, FortiMail, FortiManager, FortiSwitch, FortiOS, FortiDDoS, FortiAuthenticator, FortiMail, FortiDDoS, FortiNDR, FortiDDoS-F, FortiAuthenticator, FortiNDR, FortiWLC, FortiRecorder, FortiADC, FortiWLC, FortiTester, FortiNDR, FortiMail, FortiDDoS, FortiAnalyzer, FortiADC, FortiTester, FortiADC, FortiOS, FortiDDoS, FortiAuthenticator, FortiWLC, FortiSwitch, FortiAnalyzer, FortiNDR, FortiAuthenticator, FortiVoice, FortiTester, FortiPortal, FortiTester, FortiTester, FortiAuthenticator, FortiProxy, FortiRecorder, FortiAuthenticator, FortiOS, FortiSwitch, FortiAuthenticator, FortiSOAR, FortiVoice, FortiDDoS-F, FortiOS, FortiManager, FortiTester, FortiADC, FortiAuthenticator,	Fortinet	Jan 22, 2025, 2:21:36 PM	A externally controlled reference to a resource in another sphere in Fortinet FortiManager before version 7.4.3, FortiMail before version 7.0.3, FortiAnalyzer before version 7.4.3, FortiVoice version 7.0.0, 7.0.1 and before 6.4.8, FortiProxy before version 7.0.4, FortiRecorder version 6.4.0 through 6.4.2 and before 6.0.10, FortiAuthenticator version 6.4.0 through 6.4.1 and before 6.3.3, FortiNDR version 7.2.0 before 7.1.0, FortiWLC before version 8.6.4, FortiPortal before version 6.0.9, FortiOS version 7.2.0 and before 7.0.5, FortiADC version 7.0.0 through 7.0.1 and before 6.2.3 , FortiDDoS before version 5.5.1, FortiDDoS-F before version 6.3.3, FortiTester before version 7.2.1, FortiSOAR before version 7.2.2 and FortiSwitch before version 6.3.3 allows attacker to poison web caches via crafted HTTP requests, where the `Host` header points to an arbitrary webserver	7.2.0 <7.2.*, 6.4.0 ≤6.4.10, 6.4.0 ≤6.4.15, 5.2.0 ≤5.2.2, 6.2.0 ≤6.2.3, 5.1.0 ≤5.1.7, 7.0.0 ≤7.0.3, 7.2.0 ≤7.2.1, 7.1.0, 7.2.0 ≤7.2.2, 7.0.0 ≤7.0.13, 6.2.0 ≤6.2.13, 6.4.0 ≤6.4.1, 7.0.0 ≤7.0.1, 7.4.0 ≤7.4.2, 5.2.0 ≤5.2.8, 4.6.0, 6.1.0 ≤6.1.5, 4.1.0 ≤4.1.1, 3.6.0, 3.3.0 ≤3.3.1, 3.4.0, 1.4.0, 8.4.4 ≤8.4.8, 6.0.0 ≤6.0.12, 4.5.0, 5.1.0 ≤5.1.2, 1.0.0 ≤1.0.7, 6.0.0 ≤6.0.10, 7.0.0 ≤7.0.5, 7.2.0 ≤7.2.9, 6.4.0 ≤6.4.2, 7.0.0 ≤7.0.4, 6.2.0 ≤6.2.13, 3.7.0 ≤3.7.1, 6.0.0 ≤6.0.4, 7.0.0 ≤7.0.6, 5.3.0 ≤5.3.2, 5.3.0 ≤5.3.7,	Jan 22, 2025, 9:10:28 AM	Jan 22, 2025, 2:21:36 PM	http

					FortiDDoS, FortiProxy, FortiTester, FortiMail, FortiProxy, FortiNDR, FortiDDoS				6.4.0 ≤6.4.15, 6.4.0 ≤6.4.8, 7.4.0 ≤7.4.3, 6.0.0 ≤6.0.7, 6.2.0 ≤6.2.16, 5.0.0, 6.0.0 ≤6.0.8, 7.0.0 ≤7.0.3, 5.4.0 ≤5.4.3, 1.5.0 ≤1.5.3, 6.3.0 ≤6.3.3, 5.4.0 ≤5.4.1, 1.3.0 ≤1.3.1, 8.5.0 ≤8.5.5, 2.7.0 ≤2.7.7, 7.0.0 ≤7.0.1, 8.4.0 ≤8.4.2, 4.0.0, 1.2.0, 5.4.0 ≤5.4.12, 5.5.0 ≤5.5.1, 7.0.0 ≤7.0.13, 6.1.0 ≤6.1.6, 3.5.0 ≤3.5.1, 5.0.0 ≤5.0.4, 7.2.0, 5.1.0, 5.3.0 ≤5.3.1, 8.6.0 ≤8.6.7, 6.2.0 ≤6.2.8, 7.2.0 ≤7.2.9, 7.2.0, 6.4.0 ≤6.4.1, 6.4.0 ≤6.4.8, 3.9.0 ≤3.9.2, 6.0.0 ≤6.0.9, 3.8.0, 7.1.0 ≤7.1.1, 6.1.0 ≤6.1.3, 1.1.0 ≤1.1.6, 2.6.0 ≤2.6.3, 5.5.0, 6.4.0 <6.4.*, 7.0.0 ≤7.0.4, 6.3.0 ≤6.3.3, 6.4.3 ≤6.4.4, 6.0.0 ≤6.0.11, 6.2.0 ≤6.2.3, 6.0.0 ≤6.0.18, 6.4.0 ≤6.4.15, 4.2.0 ≤4.2.1, 5.4.0 ≤5.4.5, 6.2.0 ≤6.2.2, 4.7.0, 2.0.0 ≤2.0.14, 7.0.0, 6.2.0 ≤6.2.9,		

									1.2.0 ≤1.2.13, 1.1.0, 5.2.0			
EUVD-2024-43232	CVE-2024-48884,	Not available	v3.1: 7.1	0.06	FortiOS, FortiProxy, FortiOS, FortiProxy, FortiOS, FortiOS, FortiProxy, FortiOS, FortiProxy, FortiProxy, FortiProxy, FortiManager, FortiProxy, FortiManager	Fortinet	Jan 16, 2025, 4:15:35 PM	A improper limitation of a pathname to a restricted directory ('path traversal') in Fortinet FortiManager versions 7.6.0 through 7.6.1, 7.4.1 through 7.4.3, FortiOS versions 7.6.0, 7.4.0 through 7.4.4, 7.2.5 through 7.2.9, 7.0.0 through 7.0.15, 6.4.0 through 6.4.15, FortiProxy 7.4.0 through 7.4.5, 7.2.0 through 7.2.11, 7.0.0 through 7.0.18, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiManager Cloud versions 7.4.1 through 7.4.3 allows attacker to trigger an escalation of privilege via specially crafted packets.	7.0.0 ≤7.0.15, 7.0.0 ≤7.0.18, 7.6.0, 1.1.0 ≤1.1.6, 7.2.0 ≤7.2.9, 7.4.0 ≤7.4.4, 2.0.0 ≤2.0.14, 6.4.0 ≤6.4.15, 1.0.0 ≤1.0.7, 7.2.0 ≤7.2.11, 7.4.0 ≤7.4.5, 7.6.0 ≤7.6.1, 1.2.0 ≤1.2.13, 7.4.1 ≤7.4.3	Jan 14, 2025, 2:09:26 PM	Jan 16, 2025, 4:15:35 PM	http