



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits de Fortinet
Numéro de Référence	57521510/25
Date de publication	15 octobre 2025
Risque	Important
Impact	Important

Systemes affectés

- FortiOS toutes versions 6.0.x, 6.2.x, 6.4.x, 7.0.x, 7.2.x et 7.4.x
- FortiOS versions 7.6.x antérieures à la version 7.6.4
- FortiClientMac toutes versions 7.0.x
- FortiClientMac versions 7.2.x antérieures à la version 7.2.12
- FortiClientMac versions 7.4.x antérieures à la version 7.4.4
- FortiClientWindows toutes versions 7.0.x
- FortiClientWindows versions 7.2.x antérieures à la version 7.2.12
- FortiClientWindows versions 7.4.x antérieures à la version 7.4.4
- FortiManager Cloud toutes versions 6.4.x
- FortiManager Cloud versions 7.6.x antérieures à la version 7.6.3
- FortiManager Cloud versions postérieures à 7.0.1 et antérieures à la version 7.0.14
- FortiManager Cloud versions postérieures à 7.2.1 et antérieures à la version 7.2.10
- FortiManager Cloud versions postérieures à 7.4.1 et antérieures à la version 7.4.6
- FortiManager toutes versions 6.0.x, 6.2.x et 6.4.x
- FortiManager versions 7.0.x antérieures à la version 7.0.14
- FortiManager versions 7.2.x antérieures à la version 7.2.10
- FortiManager versions 7.4.x antérieures à la version 7.4.6
- FortiManager versions 7.6.x antérieures à la version 7.6.2
- FortiPAM toutes versions 1.0.x, 1.1.x, 1.2.x et 1.3.x
- FortiPAM versions 1.4.x antérieures à la version 1.4.3
- FortiPAM versions 1.5.x antérieures à la version 1.5.1
- FortiADC toutes versions 6.2.x et 7.0.x
- FortiADC versions 7.1.x antérieures à la version 7.1.5

- FortiADC versions 7.2.x antérieures à la version 7.2.4
- FortiADC versions 7.4.x antérieures à la version 7.4.1
- FortiAnalyzer Cloud toutes versions 6.4.x
- FortiAnalyzer Cloud versions postérieures à 7.0.1 et antérieures à la version 7.0.14
- FortiAnalyzer Cloud versions postérieures à 7.2.1 et antérieures à la version 7.2.10
- FortiAnalyzer Cloud versions postérieures à 7.4.1 et antérieures à la version 7.4.6
- FortiAnalyzer toutes versions 6.0.x, 6.2.x, 6.4.x, 7.0.x et 7.2.x
- FortiAnalyzer versions 7.4.x antérieures à la version 7.4.7
- FortiAnalyzer versions 7.6.x antérieures à la version 7.6.4
- FortiDLP toutes versions 10.3.x, 10.4.x, 10.5.x, 11.0.x, 11.1.x, 11.2.x, 11.3.x, 11.4.x, 11.5.x, 12.0.x, 12.1.x
- FortiDLP versions 12.2.x et antérieures à la version 12.2.3
- FortiIsolator toutes versions 2.3.x
- FortiIsolator versions 2.4.x antérieures à la version 2.4.5
- FortiMail versions 7.2.x antérieures à la version 7.2.7
- FortiMail versions 7.4.x antérieures à la version 7.4.3
- FortiNDR toutes versions 1.5.x, 7.0.x, 7.1.x et 7.2.x
- FortiNDR versions 7.4.x antérieures à la version 7.4.9
- FortiNDR versions 7.6.x antérieures à la version 7.6.2
- FortiProxy toutes versions 1.0.x, 1.1.x, 1.2.x, 2.0.x, 7.0.x, 7.2.x et 7.4.x
- FortiProxy versions 7.6.x antérieures à la version 7.6.4
- FortiRecorder versions 7.0.x antérieures à la version 7.0.5
- FortiRecorder versions 7.2.x antérieures à la version 7.2.2
- FortiSIEM toutes versions 6.2.x, 6.3.x, 6.4.x, 6.5.x, 6.6.x, 6.7.x, 7.0.x et 7.1.x
- FortiSIEM versions 7.2.x antérieures à la version 7.2.3
- FortiSOAR on-premise toutes versions 7.3.x et 7.4.x
- FortiSOAR on-premise versions 7.5.x antérieures à la version 7.5.2
- FortiSOAR on-premise versions 7.6.x antérieures à la version 7.6.2
- FortiSRA versions 1.4.x antérieures à la version 1.4.3
- FortiSRA versions 1.5.x antérieures à la version 1.5.1
- FortiSwitchManager versions 7.0.x antérieures à la version 7.0.4
- FortiSwitchManager versions 7.2.x antérieures à la version 7.2.6
- FortiTester toutes versions 4.2.x, 7.0.x, 7.1.x, 7.2.x et 7.3.x
- FortiTester version 7.4 antérieures à la version 7.4.3
- FortiVoice versions 6.0.7 à 6.0.12
- FortiVoice versions 6.4.x antérieures à la version 6.4.10
- FortiVoice versions 7.0.x antérieures à la version 7.0.5
- FortiWeb toutes versions 6.4.x, 7.0.x et 7.2.x
- FortiWeb versions 7.4.x antérieures à la version 7.4.5
- FortiWeb versions 7.6.x antérieures à la version 7.6.1

Identificateurs externes

CVE-2023-46718	CVE-2024-26008	CVE-2024-33507	CVE-2024-47569	CVE-2024-48891
CVE-2024-50571	CVE-2025-22258	CVE-2025-25252	CVE-2025-25253	CVE-2025-25255
CVE-2025-31365	CVE-2025-31366	CVE-2025-31514	CVE-2025-46752	CVE-2025-46774
CVE-2025-47890	CVE-2025-49201	CVE-2025-53845	CVE-2025-53950	CVE-2025-53951
CVE-2025-54658	CVE-2025-54822	CVE-2025-54973	CVE-2025-54988	CVE-2025-57716
CVE-2025-57740	CVE-2025-57741	CVE-2025-58324	CVE-2025-58325	CVE-2025-58903
CVE-2025-59921				

Bilan de la vulnérabilité

Fortinet annonce la disponibilité de mises à jour de sécurité permettant la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire d'élever ses privilèges ou de causer un déni de service.

Solution

Veillez se référer aux bulletins de sécurité de Fortinet pour mettre à jour vos produits.

Risques

- Exécution de code arbitraire
- Elévation de privilèges
- Déni de service

Références

Bulletins de sécurité de Fortinet:

- <https://www.fortiguard.com/psirt/FG-IR-23-354>
- <https://www.fortiguard.com/psirt/FG-IR-24-041>
- <https://www.fortiguard.com/psirt/FG-IR-24-062>
- <https://www.fortiguard.com/psirt/FG-IR-24-228>
- <https://www.fortiguard.com/psirt/FG-IR-24-280>
- <https://www.fortiguard.com/psirt/FG-IR-24-361>

- <https://www.fortiguard.com/psirt/FG-IR-24-372>
- <https://www.fortiguard.com/psirt/FG-IR-24-412>
- <https://www.fortiguard.com/psirt/FG-IR-24-442>
- <https://www.fortiguard.com/psirt/FG-IR-24-452>
- <https://www.fortiguard.com/psirt/FG-IR-24-457>
- <https://www.fortiguard.com/psirt/FG-IR-24-487>
- <https://www.fortiguard.com/psirt/FG-IR-24-542>
- <https://www.fortiguard.com/psirt/FG-IR-24-546>
- <https://www.fortiguard.com/psirt/FG-IR-25-010>
- <https://www.fortiguard.com/psirt/FG-IR-25-037>
- <https://www.fortiguard.com/psirt/FG-IR-25-126>
- <https://www.fortiguard.com/psirt/FG-IR-25-160>
- <https://www.fortiguard.com/psirt/FG-IR-25-198>
- <https://www.fortiguard.com/psirt/FG-IR-25-378>
- <https://www.fortiguard.com/psirt/FG-IR-25-628>
- <https://www.fortiguard.com/psirt/FG-IR-25-639>
- <https://www.fortiguard.com/psirt/FG-IR-25-653>
- <https://www.fortiguard.com/psirt/FG-IR-25-664>
- <https://www.fortiguard.com/psirt/FG-IR-25-684>
- <https://www.fortiguard.com/psirt/FG-IR-25-685>
- <https://www.fortiguard.com/psirt/FG-IR-25-756>
- <https://www.fortiguard.com/psirt/FG-IR-25-771>
- <https://www.fortiguard.com/psirt/FG-IR-25-861>