|  |
| --- |
| **Multiples vulnérabilités dans les produits Fortinet** |
| **CVE-2024-52965** **CVE-2025-24477** **CVE-2024-55599** **CVE-2025-24474** **CVE-2024-32124** **CVE-2025-47856** **CVE-2024-27779** **CVE-2025-25257** |
| **DXC MA CTI Advisory**  09/07/2025 |

Overview

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVE** | **Description** | **CVSS Score** | **Risque** | **Exploit** | **Délai de traitement** |
| **CVE-2024-52965 CVE-2025-24477 CVE-2024-55599 CVE-2025-24474 CVE-2024-32124 CVE-2025-47856 CVE-2024-27779 CVE-2025-25257** | De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. | **2.6 - 9.6** | **Atteinte à l'intégrité des données - Atteinte à la confidentialité des données - Contournement de la politique de sécurité - Exécution de code arbitraire à distance - Injection SQL (SQLi) - Élévation de privilèges** | **NON** | **2 Jr** |

Produits affectés

|  |
| --- |
| · FortiAnalyzer Cloud versions antérieures à **7.4.7** · FortiAnalyzer versions **7.6.x** antérieures à **7.6.2** · FortiAnalyzer versions antérieures à **7.4.7** · FortiIsolator versions antérieures à **2.4.5** · FortiManager Cloud versions **7.4.x** antérieures à **7.4.7** · FortiManager versions antérieures à **7.4.7** · FortiManager versions antérieures à **7.6.2** · FortiOS versions **7.2.x** et antérieures à **7.2.12** · FortiOS versions **7.4.x** antérieures à **7.4.8** · FortiOS versions **7.6.x** antérieures à **7.6.3** · FortiOS versions antérieures à **7.2.11** · FortiProxy versions **7.6.x** antérieures à **7.6.2** · FortiProxy versions **7.x** antérieures à **7.4.9** · FortiSandbox versions **4.4.x** antérieures à **4.4.5** · FortiSandbox versions antérieures à **4.2.7** · FortiVoice versions **6.4.x** antérieures à **6.4.11** · FortiVoice versions **7.0.x** antérieures à **7.0.7** · FortiVoice versions **7.2.x** antérieures à **7.2.1** · FortiWeb versions **7.0.x** antérieures à **7.0.11** · FortiWeb versions **7.2.x** antérieures à **7.2.11** · FortiWeb versions **7.4.x** antérieures à **7.4.8** · FortiWeb versions **7.6.x** antérieures à **7.6.4** |

Mitigations & Workarounds

Mettez à jour les produits Fortinet vers les versions suivantes :  
 Ø FortiAnalyzer Cloud **7.4.7** ou ultérieure  
 Ø FortiAnalyzer **7.6.2** ou ultérieure  
 Ø FortiAnalyzer **7.4.7** ou ultérieure  
 Ø FortiIsolator **2.4.5** ou ultérieure  
 Ø FortiManager Cloud **7.4.7** ou ultérieure  
 Ø FortiManager **7.4.7** ou ultérieure  
 Ø FortiManager **7.6.2** ou ultérieure  
 Ø FortiOS **7.2.12** ou ultérieure  
 Ø FortiOS **7.4.8** ou ultérieure  
 Ø FortiOS **7.6.3** ou ultérieure  
 Ø FortiOS **7.2.11** ou ultérieure  
 Ø FortiProxy **7.6.2** ou ultérieure  
 Ø FortiProxy **7.4.9** ou ultérieure  
 Ø FortiSandbox **4.4.5** ou ultérieure  
 Ø FortiSandbox **4.2.7** ou ultérieure  
 Ø FortiVoice **6.4.11** ou ultérieure  
 Ø FortiVoice **7.0.7** ou ultérieure  
 Ø FortiVoice **7.2.1** ou ultérieure  
 Ø FortiWeb **7.0.11** ou ultérieure  
 Ø FortiWeb **7.2.11** ou ultérieure  
 Ø FortiWeb **7.4.8** ou ultérieure  
 Ø FortiWeb **7.6.4** ou ultérieure

DXC MA Cyber Threat Intelligence Assessment

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Références).

Références :

|  |
| --- |
|  |
| https://www.fortiguard.com/psirt/FG-IR-24-035 https://www.fortiguard.com/psirt/FG-IR-24-045 https://www.fortiguard.com/psirt/FG-IR-24-053 https://www.fortiguard.com/psirt/FG-IR-24-437 https://www.fortiguard.com/psirt/FG-IR-24-511 https://www.fortiguard.com/psirt/FG-IR-25-026 https://www.fortiguard.com/psirt/FG-IR-25-151 https://www.fortiguard.com/psirt/FG-IR-25-250 |