|  |
| --- |
| **Multiples vulnérabilités dans OpenSSL** |
| **CVE-2025-9232** **CVE-2025-9230** **CVE-2025-9231** |
| **DXC MA CTI Advisory**  01/10/2025 |

Overview

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVE** | **Description** | **CVSS Score** | **Risque** | **Exploit** | **Délai de traitement** |
| **CVE-2025-9232 CVE-2025-9230 CVE-2025-9231** | De multiples vulnérabilités ont été découvertes dans OpenSSL. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. | **5.9 - 7.5** | **Atteinte à la confidentialité des données - Déni de service à distance - Exécution de code arbitraire à distance** | **NON** | **5 Jr** |

Produits affectés

|  |
| --- |
| · OpenSSL versions **1.0.2**x antérieures à **1.0.2**zm (support payant) · OpenSSL versions **1.1.1**x antérieures à **1.1.1**zd (support payant) · OpenSSL versions **3.0.x** antérieures à **3.0.18** · OpenSSL versions **3.2.x** antérieures à **3.2.6** · OpenSSL versions **3.3.x** antérieures à **3.3.5** · OpenSSL versions **3.4.x** antérieures à **3.4.3** · OpenSSL versions **3.5.x** antérieures à **3.5.4** |

Mitigations & Workarounds

Mise à jour OpenSSL vers les versions sécurisées:  
 Ø OpenSSL **1.0.2**zm ou ultérieure  
 Ø OpenSSL **1.1.1**zd ou ultérieure  
 Ø OpenSSL **3.0.18** ou ultérieure  
 Ø OpenSSL **3.2.6** ou ultérieure  
 Ø OpenSSL **3.3.5** ou ultérieure  
 Ø OpenSSL **3.4.3** ou ultérieure  
 Ø OpenSSL **3.5.4** 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://openssl-library.org/news/secadv/20250930.txt |