Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0005

Kwetsbaarheden verholpen in Ivanti Connect Secure en Policy Secure

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 17-01-2025
Revisie: 1.0.5

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 5

Ivanti adviseert om de interne en externe Integrity Checker Tools (ICT) te gebruiken op betreffende apparatuur, de interne integrity check tool zou echter mogelijk door malafide handelingen niet correct werken. Uit open bronnen blijkt dat er antiforensische methoden zouden zijn toegepast welke, bij eerder misbruik, niet enkel met een patch zouden kunnen worden opgelost.

Feiten

Ivanti heeft kwetsbaarheden verholpen in Connect Secure en Policy Secure.

Duiding

De eerste kwetsbaarheid (CVE-2025-0282) kan door kwaadwillenden misbruikt worden om zonder authenticatie op afstand willekeurige code uit te voeren. De tweede kwetsbaarheid (CVE-2025-0283) kan door een lokaal geauthenticeerde kwaadwillende misbruikt worden om de rechten te verhogen.

Ivanti geeft aan dat CVE-2025-0282 actief misbruikt word bij gebruikers van Connect Secure. Er is Proof-of-Concept-code beschikbaar.

Ivanti adviseert om de interne en externe Integrity Checker Tools (ICT) te gebruiken op betreffende apparatuur, de interne integrity check tool zou echter mogelijk door malafide handelingen niet correct werken. Het NCSC adviseert om de meest recente versies van de Integrity Checker Tools (ICT) in te zetten om mogelijk misbruik te kunnen detecteren. Op dit moment is dat versie ICT-V22725 (build 3819).

In de aanval zouden mogelijk meerdere persistence technieken zijn toegepast, een daarvan is het blokkeren van een legitieme patch en in plaats daarvan een schijn patch op het scherm weer te geven als het systeem gepatched wordt. Dit zou betekenen dat de update die zou zijn uitgevoerd niet correct is en mogelijk zou een kwaadwillende nog steeds toegang hebben tot het apparaat. Ook adviseert Ivanti om bij onderkenning van eerder misbruik betreffende apparatuur te factory resetten en de versie terug te zetten naar 22.7R2.5. Het is belangrijk dat bij tekenen van misbruik credentials en API tokens worden geroteerd, deze zouden mogelijk gestolen kunnen zijn.

Oplossingen

Ivanti heeft patches uitgebracht om de kwetsbaarheid te verhelpen in Connect Secure versie 22.7R2.5. Gebruikers van Connect Secure worden daarnaast door Ivanti dringend geadviseerd om de integriteit van het systeem met de interne en externe Integrity Checker Tools (ICT) te onderzoeken. Hiermee kunnen mogelijke antiforensische handelingen worden gedetecteerd.

Voor Policy Secure zal naar verwachting op 21 januari een patch beschikbaar komen. Dit product hoort echter normaliter niet via het internet bereikbaar te zijn en er is dan ook geen actief misbruik van de kwetsbaarheden in Policy Secure bekend.

Google TI heeft een blog geschreven over het misbruik met meerdere indicators of compromise (IoC's) welke kunnen ondersteunen bij onderzoek.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US
- https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-0282	9.0 CRITICAL
CVE-2025-0283	7.0 HIGH

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow

Getroffen producten

ivanti
connect_secure
policy_secure

Disclaimer