Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0484

Kwetsbaarheden verholpen in Ivanti Connect Secure en Policy Secure

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-12-2024
Revisie: 1.0.1

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 1

NCSC ontvangt uit betrouwbare bron informatie dat de kwetsbaarheden beperkt zijn misbruikt.

Feiten

Ivanti heeft kwetsbaarheden verholpen in Ivanti Connect Secure (Specifiek voor versies vóór 22.7R2.4) en Policy Secure (Specifiek voor versies vóór 22.7R1.2).

Duiding

De kwetsbaarheden bevinden zich in de Secure Application Manager component en de IPSEC-component van Ivanti Connect Secure en Policy Secure en omvatten onvoldoende server-side controles. Deze kwetsbaarheden kunnen worden misbruikt door kwaadwillenden om beveiligingsrestricties te omzeilen en ongeautoriseerde controle over de systemen te verkrijgen of een Denial-of-Service te veroorzaken. Dit kan leiden tot een inbreuk op de beveiligingsarchitectuur van de getroffen organisaties.

De kwetsbaarheden bevinden zich (m.u.v. CVE-2024-11634) ook in de systeemversie 9.x. Deze is echter sinds juni 2024 End-of-Engineering en zal per 31 december 2024 End-of-Life gaan, waardoor deze géén updates zal ontvangen om deze kwetsbaarheden te verhelpen.

De kwetsbaarheden met kenmerk CVE-2024-37377 en CVE-2024-37401 bevinden zich in de IPSEC-functionaliteit en zijn op afstand te misbruiken zonder voorafgaande authenticatie. Succesvol misbruik leidt tot een Denial-of-Service (DoS).

De kwetsbaarheid met kenmerk CVE-2024-9844 bevindt zich in de Secure Application Manager en vereist voorafgaande authenticatie. De kwetsbaarheden met kenmerk CVE-2024-11633 en CVE-2024-11634 vereisen voorafgaande authenticatie met Admin-rechten. Misbruik van deze kwetsbaarheden stelt een kwaadwillende in staat om willekeurige code uit te voeren op het kwetsbare systeem.

Uit betrouwbare bron ontvangt het NCSC signalen dat de kwetsbaarheden beperkt zijn misbruikt. Er is geen publiek beschikbare Proof-of-Concept (PoC) of exploitcode beschikbaar. Het is mogelijk dat deze wel op korte termijn beschikbaar komt, waarmee de kans op grootschalig misbruik toeneemt.

Oplossingen

Ivanti heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Connect Secure 22.7R2.4 en Policy Secure 22.7R1.2. Versie 9.x van zowel ICS als PCS zijn per 31 december 2024 End-of-Life en hebben daarom géén updates ontvangen. Ivanti adviseert om z.s.m. over te gaan naar de ondersteunde versie 22.7 van beide systemen. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Connect-Secure-ICS-and-Ivanti-Policy-Secure-IPS-Multiple-CVEs

Kwetsbaarheden

CVE	CVSS Score
› CVE-2024-9844	7.1 HIGH
› CVE-2024-11633	9.1 CRITICAL
› CVE-2024-11634	9.1 CRITICAL
› CVE-2024-37377	7.5 HIGH
› CVE-2024-37401	7.5 HIGH

CWE's

CWE	Beschrijving
› CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
› CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
› CWE-602	Client-Side Enforcement of Server-Side Security

Getroffen producten

ivanti
connect_secure
policy_secure

Disclaimer