2024-038 CERT-Hessen Warnmeldung

16.08.2024, 10:15 Uhr

Umgehung der Authentifizierung in Ivanti Virtual Traffic Manager (vTM)

Tags: Schwachstelle | Patch | vTM | Layer 7 | Invanti

Sachverhalt:

Die Schwachstelle CVE-2024-7593 (CVSS-Score von 9.8/10) ermöglicht einem nicht authentifizierten Angreifer aus der Ferne, die Authentifizierung zu umgehen und einen administrativen Account zu erstellen, was zu einer vollständigen Systemkompromittierung führen könne. Ursache ist die fehlerhafte Implementierung eines Authentifizierungsalgorithmus.

Betroffene Produkte:

Ivanti vTM Versionen < 22.2R1 | 22.7R2

Bewertung:

Hessen3C bewertet den Angriff als kritisch, da die Schwachstelle zur Übernahme eines fremden IT-System aus dem Internet verwendet werden kann.

Empfehlung von Maßnahmen

Hessen3C empfiehlt die Updates des Herstellers einzuspielen, wenn diese zur Verfügung stehen.

Ergänzend sollte entsprechend der Herstellerempfehlung geprüft werden, ob Zugriffe von externen Netzen auf administrative Bereiche bis zur Bereitstellung eines Sicherheitsupdates deaktiviert werden können.

Weitere Quellen

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2024-7569-CVE-2024-7570?language=en_US

Hessen3C

Kurzfassung: Bedeutung der Traffic Light Protocol-Einstufungen

TLP:CLEAR: Unbegrenzte Weitergabe
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

TLP:GREEN: Organisationsübergreifende Weitergabe
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der CybersecurityCommunity) angehören.

TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

> TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
> Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

TLP:RED: Persönlich, nur für benannte Empfänger Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

Eine ausführliche Erläuterung zum Traffic-Light-Protokoll finden Sie im Dokument „*CERT-Verpflichtung-TLP.pdf*“ unter http://www.cert.hessen.de

Kontaktdaten:
Hessen CyberCompetenceCenter (Hessen3C)

Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz
Friedrich-Ebert-Allee 12
65185 Wiesbaden

Telefon, Notrufhotline: **+49 (611) 353 9900**
Fax: +49 (611) 353 1919
E-Mail: **cert@hessen3c.hessen.de**
Website: **https://www.hessen3c.de**