



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

VMware vCenter Server Plugin mit kritischer RCE-Schwachstelle (CVE-2021-21972)

CSW-Nr. 2021-189544-1132, Version 1.1, 11.03.2021

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

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

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Für eine von der Firma PT Security gemeldete kritische Remote Code Execution (RCE) Schwachstelle (CVE-2021-21972) in einem VMware vCenter Server Plugin [SWA2021] wurden mittlerweile verschiedene Proof-of-Concept Exploit Codes veröffentlicht (siehe auch [PST2021] [GIT2021a] [GIT2021b] [GIT2021c]).

VMware vCenter Server werden von IT-Administratoren verwendet, um in VMware Infrastrukturen mehrere Virtualisierungs-Server, virtuelle Maschinen, Speicher und Netzwerk zu verwalten.

Die Ausnutzung der referenzierten Schwachstelle ermöglicht es einem nicht authentifizierten Angreifer mit Netzwerkzugriff auf den TLS-/SSL-Port 443 des vCenter-Servers, administrative Rechte zu erlangen und auf dem zugrundeliegenden Betriebssystem beliebigen Programmcode auszuführen. Die Schwachstelle CVE-2021-21972 wurde von VMware mit einem Common Vulnerability Scoring System (CVSS) v3 Wert von 9.8 bewertet (siehe [VMW2021]) und betrifft die folgenden Produktversionen:

- * 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Version	Patchlevel
vCenter Server 6.5	< 6.5 U3n
vCenter Server 6.7	< 6.7 U3l
vCenter Server 7.0	< 7.0 U1c

Bewertung

Dem BSI liegen zurzeit keine Informationen bzgl. einer aktiven Ausnutzung der Schwachstelle vor. Allerdings gibt es Hinweise darauf, dass im Internet bereits nach verwundbaren VMware vCenter-Servern gescannt wird (siehe [TWI2021]). Da bereits verschiedene Proof-of-Concept (PoC) Codes veröffentlicht wurden, dürfte die Verfügbarkeit eines funktionierenden Exploits nur eine Frage der Zeit sein.

Die Schwachstelle ist von hoher Relevanz, da sie in der Grundkonfiguration des vCenter Managers vorliegt und eine vollständige Kompromittierung betroffener Systeme ermöglicht. Gleichwohl sollten vCenter-Instanzen prinzipiell nicht so konfiguriert sein, dass sie aus dem Internet erreichbar sind.

Die Kritikalität der Schwachstelle wird durch die Art und Weise begünstigt, wie VMware vCenter die VMware Infrastruktur an zentraler Stelle miteinander verbindet. Nach einer erfolgreichen Kompromittierung des vCenter-Servers ist potenziell der Zugriff auf die verwalteten Virtualisierungs-Server, die virtuellen Maschinen, den zentralen Datenspeicher sowie das Netzwerk möglich.

Maßnahmen

Das BSI empfiehlt dringend, die aktuelle Version der vCenter-Software einzuspielen. Die aktuellen Sicherheitspatches können über das offizielle VMware Patch Download Center bezogen bzw. über die integrierte Update-Funktion des vCenter-Servers installiert werden (siehe [VMW2021a]). Sollte der Wechsel auf einen sicheren Versionsstand der Software nicht unmittelbar möglich sein, empfiehlt der Hersteller zeitnah einen temporären Workaround umzusetzen (siehe [VMW2021b]), bis die Sicherheitspatches installiert werden können.

VMware vCenter-Server sollten aus einem separaten, besonders gehärteten Management-Netz heraus verwendet werden. Ergänzend ist die Umsetzung weiterer Maßnahmen aus dem IT-Grundschutzkompendium zu prüfen (siehe [BSI2021]).

Links

[BSI2021] - Grundschutzkompendium Server SYS.1.5: Virtualisierung (Edition 2021)

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium Einzel PDFs 2021/07 SYS IT Systeme/SYS 1 5 Virtualisierung Edition 2021.html>

[GIT2021a] - CVE-2021-21972 Proof Of Concept

<https://github.com/yaunsky/CVE-2021-21972/blob/main/CVE-2021-21972.py>

[GIT2021b] - CVE-2021-21972-vCenter-6.5-7.0-RCE-POC

<https://github.com/QmF0c3UK/CVE-2021-21972-vCenter-6.5-7.0-RCE-POC/blob/main/CVE-2021-21972.py>

[GIT2021c] - CVE-2021-21972 Proof Of Concept

<https://github.com/NS-Sp4ce/CVE-2021-21972/blob/main/CVE-2021-21972.py>

[PST2021] - VMware vCenter 6.5 / 7.0 Remote Code Execution Proof Of Concept

<https://packetstormsecurity.com/files/161527/CVE-2021-21972.py.txt>

[SWA2021] - PT SWARM Unauthorized RCE in VMware vCenter Exploit Advisory

<https://swarm.ptsecurity.com/unauth-rce-vmware/>

[TWI2021] - Bad Packets Tweet

https://twitter.com/bad_packets/status/1364661586070102016

[VMW2021] - VMware Security Advisory zu CVE-2021-21972

<https://www.vmware.com/security/advisories/VMSA-2021-0002.html>

[VMW2021a] - VMware Patch Download Center

<https://my.vmware.com/group/vmware/patch>

[VMW2021b] - VMware vCenter Server Workaround zu CVE-2021-21972

<https://kb.vmware.com/s/article/82374>

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

- 1) Was ist das Traffic Light Protokoll?
Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensiblen Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.
- 2) Welche Einstufungen existieren?
 - **TLP:WHITE: Unbegrenzte Weitergabe**
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
 - **TLP:GREEN: Organisationsübergreifende Weitergabe**
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
 - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. 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. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
- 3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
- 4) Was passiert, wenn ich die Einstufung nicht beachte?
Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.