



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in VMware vCenter Standard Server Installation (CVE-2021-22005)

CSW-Nr. 2021-252248-1032, Version 1.0, 22.09.2021

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

VMware vCenter Server ist eine Servermanagementsoftware, welche von IT-Administratoren verwendet wird, um in VMware Infrastrukturen mehrere Virtualisierungs-Server, virtuelle Maschinen, Speicher und Netzwerke zu verwalten.

Am 21. September 2021 veröffentlichte das Unternehmen VMware Inc. Informationen zu insgesamt 19 Schwachstellen in den Produkten VMware vCenter Server (vCenter Server) und VMware Cloud Foundation (Cloud Foundation) [VMW2021a]. Die beschriebenen Sicherheitslücken wurden nach CVSS v3 (Common Vulnerability Scoring System) mit verschiedenen Kritikalitäten bewertet. Von besonderer Tragweite ist dabei vor allem die Schwachstelle CVE-2021-22005, die mit einem Wert von 9.8 als "kritisch" eingestuft wurde. Hierbei handelt es sich um eine Sicherheitslücke im Uploadservice des Analytics Service des VMware vCenter Servers der Versionen 6.7 und 7.0 [MIT2021] sowie in den Versionen 4.x der Cloud Foundation. Ein nicht authentifizierter Angreifer mit Netzwerkzugriff auf den TLS-/SSL-Port 443 des VMware vCenter Servers hat dabei die Möglichkeit, eine manipulierte Datei hochzuladen um beliebigen Programmcode auf Betriebssystemebene ausführen zu können.

* 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.

Bewertung

Dem BSI liegen zurzeit keine Informationen bzgl. einer aktiven Ausnutzung der Schwachstellen vor. VMware weist jedoch in einem Statement darauf hin, dass man sehr kurzfristig mit einer Ausnutzung und der Veröffentlichung von Exploit-Code rechnen [VMW2021d].

Die Schwachstellen sind von hoher Relevanz, da sie in der Grundkonfiguration des VMware vCenter Servers vorliegen und eine vollständige Kompromittierung betroffener Systeme ermöglichen. Die Kritikalität wird durch die Art und Weise begünstigt, wie VMware vCenter Server 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.

Bereits im Juni 2021 warnte das BSI entsprechend vor verwundbaren VMWare ESXi-Servern im Zusammenhang mit Ransomware-Angriffen.

Maßnahmen

Das BSI empfiehlt dringend, die aktuelle Version des VMware vCenter Servers einzuspielen, die am 21.09.2021 vom Hersteller veröffentlicht worden ist. Die aktuellen Sicherheitspatches können über das offizielle VMware Patch Download Center bezogen bzw. über die integrierte Update-Funktion des vCenter-Servers installiert werden (siehe [VMW2021b]). Sollte der Wechsel auf einen sicheren Versionsstand der Software nicht unmittelbar möglich sein, empfiehlt der Hersteller zeitnah einen temporären Workaround umzusetzen (siehe [VMW2021c]), bis die Sicherheitspatches installiert werden können.

Das BSI empfiehlt zusätzlich die unten aufgeführten Maßnahmen umzusetzen, um einen umfangreichen Schutz in der Umgebung zu gewährleisten:

- Legen Sie Offline-Backups an und speichern Sie auch die Logdaten der VMWare ESXi-Server sicher auf zentralen Systemen ab.
- Deaktivieren Sie SSH auf den VMWare ESXi-Servern oder filtern Sie den Zugriff (z.B. per Firewall).
- Trennen Sie strikt zwischen VMWare-Administrationskonten und Microsoft Windows Domain-Administrationskonten.
- Führen Sie eine Netzwerksegmentierung mit restriktiven Paketfiltern ein (z.B. Administrationsnetzwerk, Arbeitsnetzwerk, Server-Netzwerk, etc.) und verwalten Sie VMware vCenter-Server aus einem separaten, besonders gehärteten Management-Netz heraus (siehe [BSI2021a]).
- Verboten Sie den direkten Internetzugriff von Administrations-Arbeitsplätzen aus.
- Verwenden Sie unterschiedliche Rechner und Accounts für die Administration und die normalen Arbeitsprozesse des IT-Personals.
- Ergänzend ist die Umsetzung weiterer Maßnahmen aus dem IT-Grundschutz-Kompendium zu prüfen (siehe [BSI2021b]).

Links

[BSI2021a] - NET.1.1: Netzarchitektur und -design (Edition 2021)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium Einzel PDFs 2021/09_NET_Netze_und_Kommunikation/NET_1_1_Netzarchitektur_und_design_Edition_2021.html

[BSI2021b] - IT-Grundschutz-Kompendium 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

[MIT2021] - Critical vCenter Server File Upload Vulnerability CVE-2021-22005

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22005>

[TWI2021] - Tweet von CERT-Bund

<https://twitter.com/certbund/status/1400364158273699843>

[VMW2021a] - VMware Advisory VMSA-2021-0020

<https://www.vmware.com/security/advisories/VMSA-2021-0020.html>

[VMW2021b] - VMware Patch Download Center

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

[VMW2021c] - VMware vCenter Server Workaround zu CVE-2021-22005

<https://kb.vmware.com/s/article/85717>

[VMW2021d] - VMSA-2021-0020: Questions & Answers

<https://core.vmware.com/vmsa-2021-0020-questions-answers-faq>

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 sensitiven 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.