Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kombinierte Ausnutzung kritischer Schwachstellen kann die Übernahme von ausgewählten VMWare-Produkten ermöglichen

CSW-Nr. 2022-224205-1032, Version 1.0, 19.05.2022

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

Am 18.05.2022 veröffentlichte das Unternehmen VMWare mit dem Security-Advisory VMSA-2022-0014 Informationen zu zwei kritischen Schwachstellen in verschiedenen VMWare Produkten (siehe [VMW2021a]). Die Schwachstellen CVE-2022-22972 und CVE-2022-22973 können es Angreifenden durch eine kombinierte Ausnutzung ermöglichen, sich ohne Authentisierung administrativen Zugang mit Root-Rechten zu verschaffen (siehe [CISA2022b]). Betroffen durch diese beiden Schwachstellen sind die Produkte

- VMware Workspace ONE Access (Access) (Version <= 21.08.0.1),
- VMware Identity Manager (vIDM) (Version <= 3.3.6),
- VMware vRealize Automation (vRA) (Version <= 7.6),
- VMware Cloud Foundation (Version <= 4.3.x),
- vRealize Suite Lifecycle Manager (Version <= 8.x).

* 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.

Bei der CVE-2022-22972 handelt es sich um eine Schwachstelle zur Umgehung der Authentifizierung (Authentication Bypass), die es einem Angreifenden mit Netzwerkzugriff über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) der VMWare Produkte erlaubt, administrativen Zugang zu erlangen, ohne sich authentisieren zu müssen (siehe [MIT2022a]). CVE-2022-22973 ermöglicht eine lokale Rechteausweitung (Local Privilege Escalation), mit der sich lokale Angreifende Root-Rechte verschaffen können (siehe [MIT2022b).

Nach dem Common Vulnerability Scoring System (CVSS) wird der Schweregrad der Sicherheitslücken mit 9.8 als "kritisch" (CVE-2022-22972) bzw. mit 7.8 als "hoch" (CVE-2022-22973) eingestuft (CVSSv3).

Die amerikanische Cybersecurity & Infrastructure Security Agency (CISA) berichtete am 18.05.2022, dass es Angreifenden (darunter auch Advanced Persistent Threat (APT)-Gruppen) gelungen sei, die bereits im April gepatchten Schwachstellen CVE-2022-22954 und CVE-2022-22960 auszunutzen (siehe [CISA2022a]). Auf Basis dieser Erfahrungen geht CISA davon aus, dass auch CVE-2022-22972 und CVE-2022-22973 zeitnah ausgenutzt werden könnten (siehe [CISA2022a], [CISA2022b]).

Bewertung

Dem BSI liegen zurzeit keine Informationen bzgl. einer aktiven Ausnutzung der veröffentlichten Schwachstellen vor.

Grundsätzlich sollte die DCUI nicht aus dem Internet erreichbar sein. Daher ist diese Option auch standardmäßig vom Hersteller deaktiviert. Ist dies nicht der Fall, ist angeraten, das entsprechende Gerät unverzüglich vom Netz zu trennen und das Netzwerk auf Anomalien zu überprüfen. Die CISA stellt entsprechende Snort Signaturen, YARA Regeln und Indicators of Compromise (IoC) zur Verfügung (siehe [CISA2022b]).

Maßnahmen

Das BSI empfiehlt dringend, die aktuelle Version der VMWare Produkte einzuspielen. Sicherheitspatches können über das offizielle VMware Patch Download Center bezogen werden (siehe [VMW2022a]). Sollte der Wechsel auf einen sicheren Versionsstand der Software nicht unmittelbar möglich sein, empfiehlt der Hersteller, zeitnah einen temporären Workaround umzusetzen (siehe [VMW2022a]), bis die Sicherheitspatches installiert werden können. Der Hersteller hat zusätzlich eine FAQ-Webseite zu den Schwachstellen bereitgestellt (siehe [VMWare2022b]).

Ergänzend ist die Umsetzung weiterer Maßnahmen aus dem IT-Grundschutz-Kompendium zu prüfen (siehe [BSI2022a]).

Wenn Sie sich bezüglich einer möglichen Kompromittierung durch eine APT-Gruppe unsicher sind, wenden Sie sich an einen der vom BSI qualifizierten Dienstleister: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf

Links

[VMWare2022a] VMSA-2022-0014, https://www.vmware.com/security/advisories/VMSA-2022-0014.html

[VMWare2022b] VMSA-2022-0014: Questions & Answers, https://core.vmware.com/vmsa-2022-0014-questions-answers-faq

[CISA2022a] Emergency Directive 22-03 Mitigate VMware Vulnerabilities, https://www.cisa.gov/emergency-directive-22-03

[CISA2022b] Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control, https://www.cisa.gov/uscert/ncas/alerts/aa22-138b

[MIT2022a] CVE- CVE-2022-22972,https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22972

[MIT2022b]CVE - CVE-2022-22973 ,https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22973

[BSI2022a] IT-Grundschutz: Baustein SYS.1.5 Virtualisierung (Edition 2022), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/07_SYS_IT_Systeme/SYS_1_5_Virtualisierung_Edition_2022.pdf

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.