Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Schwachstelle in VMware ESXi weltweit massiv ausgenutzt

CSW-Nr. 2023-205338-1232, Version 1.2, 08.02.2023

IT-Bedrohungslage*: 3 / Orange

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:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR 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

Bei einem weltweit breit gestreuten Angriff wurden laut Medienberichten tausende Server, auf denen VMwares Virtualisierungslösung ESXi zum Einsatz kommt, mit Ransomware infiziert [REU2023] und verschlüsselt. Die regionalen Schwerpunkte der Angriffe lagen dabei auf Frankreich, den USA, Deutschland und Kanada - auch weitere Länder sind betroffen. Die Täter machten sich eine länger bekannte Schwachstelle im OpenSLP Service der Anwendung zu Nutze, bei der ein "Heap Overflow" angestoßen und dadurch letztendlich Code aus der Ferne ausgeführt werden kann.

Informationen zur Sicherheitslücke selbst – die als CVE-2021-21974 geführt und nach CVSS mit einem Schweregrad von 8.8 als "hoch" bewertet wird – sowie ein Patch wurden vom Hersteller bereits im Februar 2021 veröffentlicht. Auf die dazugehörige Meldung von VMware [VMW2021] hatte auch das BSI damals über seine verschiedenen Kanäle hingewiesen [BSI2021].

Konkretere Aussagen zur Betroffenheit und zum Ausmaß möglicher Schäden sind derzeit noch nicht möglich. Das BSI analysiert diesen IT-Sicherheitsvorfall jedoch intensiv und steht im engen Austausch mit seinen internationalen Partnern. Sobald neue Informationen vorliegen, wird das BSI über aktuelle Erkenntnisse sowie Schutzmöglichkeiten informieren.

* 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.

Update 1:
VMware hat sich zu den Beobachtungen der vergangenen Tage geäußert [VMW2023]. Dabei stellt das Unternehmen fest, dass für die Angriffe nach bisherigen Erkenntnissen ausschließlich Schwachstellen genutzt werden, die bereits länger bekannt sind. Eine detailliertere Spezifikation erfolgte jedoch nicht. Insofern kann nicht ausgeschlossen werden, dass neben CVE-2021-21974 auch andere, bereits gepatchte Sicherheitslücken zum Einsatz kommen.

Während derzeit Vieles darauf hinweist, dass bereits infizierte Systeme aufgrund der fehlerfreien Verschlüsselung nicht mehr wiederhergestellt werden können [BPC2023], gelang möglicherweise die Bereinigung in vereinzelten Fällen auf Basis der hier beschriebenen Vorgehensweise [ENE2023].

Definitiv bestätigt sind hingegen Attacken auf Ziele in Deutschland. In dieser Woche meldeten sich mehrere deutsche Institutionen beim BSI, nachdem Angriffe auf deren Server stattgefunden hatten. Das BSI wird diese Meldungen nun weiter prüfen.
Gleichzeitig nahm die Anzahl der potenziell verwundbaren Ziele in Deutschland ab. Dies deutet darauf hin, dass diese Systeme zwischenzeitlich gepatcht oder bzgl. ihrer Erreichbarkeit aus dem Internet eingeschränkt wurden.

Update 2:
Eine detaillierte Analyse der ESXiArgs Angriffe sowie Hinweise auf eine Kompromittierung können [CYB2023] entnommen werden.

Außerdem hat die amerikanische Cybersecurity and Infrastructure Security Agency (CISA) am Abend des 7. Februar ein Skript zur Verfügung gestellt, das ausgewählte kompromittierte Systeme wiederherstellen kann [GIT2023]. Dieses basiert u.a. auf den Erkenntnissen von [ENE2023].
In diesem Zusammenhang bestätigte das französische CERT (CERT-FR), dass insbesondere dann eine Chance zur Wiederherstellung bestehe, wenn lediglich Konfigurationsdateien (.vmdk) verschlüsselt und mit der Erweiterung .args umbenannt wurden. Mehrere erfolgreich erprobte Verfahren seien dokumentiert [CFR2023].

Bewertung

Die massenhafte Ausnutzung der Schwachstelle durch Ransomware kann zu erheblichen Beeinträchtigungen der Abläufe in zahlreichen Organisationen führen. Dies betrifft nicht nur diejenigen Institutionen, die VMware ESXi selbst einsetzen und verschlüsselt wurden, sondern auch dritte Organisationen. Zum Beispiel dann, wenn ein Geschäftspartner vereinbarte Leistungen aufgrund eines Verfügbarkeits-Vorfalls kurzfristig nicht liefern kann.

Gleichzeitig unterstreicht der Sachverhalt einmal mehr die dringende Notwendigkeit eines funktionierenden Patchmanagements. Der Softwarehersteller hatte bereits im Februar 2021 auf die Schwachstelle hingewiesen und einen Patch veröffentlicht. Organisationen, die jetzt noch verwundbar sind, sollten die Schwachstelle kurzfristig schließen und ihre internen Prozesse zum Patchmanagement verbessern.

Auch sollte nochmal die Notwendigkeit und Art der Erreichbarkeit eigener Systeme aus dem Internet bzw. Intranet überprüft werden.

Mögliche Auswirkungen auf Kritische Infrastrukturen inkl. Verwaltung

Der geschilderte Vorfall kann auch Kritische Infrastrukturen treffen und die dargestellten Konsequenzen haben.

Fragen an IT-Sicherheitsverantwortliche

- Kommt in Ihrer Institution VMware ESXi in einer der folgenden Versionen zum Einsatz?
  - › ESXi 7.x-Versionen vor ESXi70U1c-17325551
  - › ESXi-Versionen 6.7.x früher als ESXi670-202102401-SG

› ESXi-Versionen 6.5.x früher als ESXi650-202102101-SG

- Ist die Installation des Patches kurzfristig möglich?
  Sofern keine Installation möglich ist: Wurden die unter [VMW2021] beschrieben Workarounds oder andere Maßnahmen zur "Nichterreichbarkeit" / sicheren Erreichbarkeit der Systeme umgesetzt?
- Stehen Backups für die Daten zur Verfügung, die auf den potenziell betroffenen Systemen gespeichert sind? Sind Ihre Backups grundsätzlich gegen Verschlüsselungsangriffe "offline" gesichert?!
- Werden bei Verwundbarkeit / offener Lücke und (noch) nicht erfolgter Verschlüsselung Log-Dateien auf verdächtige Systemzugriffe untersucht, um eine zwischenzeitlich erfolgte Infektion auszuschließen?
- Sind die vom BSI empfohlenen Maßnahmen zu Ransomware im Allgemeinen bekannt? [BSI2023a]
- Kann das Patchmanagement in Ihrer Institution optimiert werden? [BSI2023b]

Update 1:

- Unabhängig vom hier beschriebenen Sachverhalt: Sind ausschließlich solche Schnittstellen gegenüber dem Internet exponiert, die notwendigerweise aus dem Internet erreichbar sein müssen? [BSI2023c]

Links

[BPC2023]Massive ESXiArgs ransomware attack targets VMware ESXi servers worldwide:
https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

[BSI2021] VMware vCenter Server Pluginmit kritischer RCE-Schwachstelle(CVE-2021-21972):
https://bsi.bund.de/dok/894550

[BSI2023a] Ransomware:Fortschrittliche Angriffe – dynamische Entwicklung:
https://bsi.bund.de/dok/522730

[BSI2023b] BSI IT-Grundschutz: OPS 1.1.3 – Patch- und Änderungsmangement (Edition 2023):
https://bsi.bund.de/dok/1073628

[BSI2023c] BSI IT-Grundschutz: NET.3.2 Firewall (Edition 2023):
https://bsi.bund.de/dok/1073490

[CFR2023] Bulletin d'alerte du CERT-FR - Objet: [MàJ] Campagne d’exploitation d’une vulnérabilité affectant VMware ESXi:
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/

[CYB2023]Massive Ransomware Attack Targets VMware ESXi Servers:
https://blog.cyble.com/2023/02/06/massive-ransomware-attack-targets-vmware-esxi-servers/

[ENE2023]Decrypt your *.vmdk affected by CVE-2020-3992 / CryptoLocker attack:
https://enes.dev/

[GIT2023] ESXiArgs-Recover:
https://github.com/cisagov/ESXiArgs-Recover

[REU2023]Italy warns hackers targeting known server vulnerability:
https://www.reuters.com/world/europe/italy-sounds-alarm-large-scale-computer-hacking-attack-2023-02-05/

[VMW2021] VMware Advisory VMSA-2021-0002:
https://www.vmware.com/security/advisories/VMSA-2021-0002.html

[VMW2023]VMware Security Response Center (vSRC) Response to ‘ESXiArgs’ Ransomware Attacks:
https://blogs.vmware.com/security/2023/02/83330.html

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 vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **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 Cybersecurity-Community) 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.

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:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.