Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Microsoft Azure mit kritischer Sicherheitslücke

Nr. 2021-252113-1022, Version 1.0, 20.09.2021

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

Analysten der das Thema Cloud-Sicherheit behandelnden Firma WIZ entdeckten mehrere Schwachstellen über die virtuelle Linux Maschinen der Cloud-Plattform Azure angreifbar sind [WIZ2021]. Die Schwachstellen betreffen die von Azure eingesetzte Managementlösung Open Management Infrastructure (OMI) und werden unter dem Namen OMIGOD zusammengefasst. Den höchsten Score hat mit 9.8 (CVSS3.0) die Schwachstelle CVE-2021-38647 (unauthentifizierte Remote Code Execution mit Root-Rechten über eine simple Netzwerkanfrage). Mit den übrigen Sicherheitslücken ist jeweils eine Privilegieneskalation möglich.

OMI wird auf Linux VMs in Azure automatisch installiert wenn einer oder mehrere der folgenden Dienste mit der VM genutzt werden:

- Azure Automation
- Azure Automatic Update
- Azure Operations Management Suite (OMS)
- Azure Log Analytics
- Azure Configuration Management
- Azure Diagnostics

* 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.

Eine Maschine bzw. der darauf installierte Agent ist üblicherweise über die Netzwerkports 5985, 5986 und 1270 erreichbar.

Bewertung

Das Risiko einer Ausnutzung der Schwachstellen wird wegen der einfachen Ausnutzung, der Möglichkeit von Remote Code Execution mit Root-Rechten und dem möglichen Effekt für die Cloud-Umgebung als kritisch gewertet [CER2021]. Vorbedingung ist die Erreichbarkeit über das Internet. Innerhalb eines Kontos bei Azure ist die Schwachstelle schwerwiegender wenn ein Angreifer über andere Schwachstellen wie bspw. Konfigurationsfehler oder weitere ungepatchte, angreifbare Software zusätzlich verfügen kann.

Es wurde eine gepatchte Version von OMI veröffentlicht. Diese muss aber manuell vielen Fällen manuell installiert werden. Zumindest zeitweise wurde von Microsoft beim Erstellen einer Linux-VM auch weiterhin die verwundbare Version ausgerollt.

Die Schwachstellen werden laut Medienmeldungen [BLE2021] inzwischen ausgenutzt. VMs werden hiernach aktuell mit Schadcode infiziert um sie bspw. als Bot oder Cryptominer zu missbrauchen.

Maßnahmen

Der OMI Agent muss mindestens in der Version 1.6.8-1 installiert sein. Administratoren wird dringend dazu geraten, auf Linux-VMs die Version des installierten OMI Agenten zu validieren. Ob der OMI Agent auf einer Linux-VM vorhanden ist, kann mit dem folgenden Befehl erkannt werden:

```
adminuser@linux-vm:~$ sudo dpkg -l omi
dpkg-query: no packages found matching omi
```

Das entsprechende Update ist nach der Anweisung von Microsoft [MSR2021] zu installieren. Hier finden sich auch Informationen darüber, für welche Systeme manuelle Updates benötigt werden, wie verwundbare Systeme erkannt und wie das Ausnutzen der Schwachstellen detektiert werden kann.

Links

[WIZ2021] Secret Agent Exposes Azure Customers to Unauthorized Code Execution
https://www.wiz.io/blog/secret-agent-exposes-azure-customers-to-unauthorized-code-execution

[CER2021] Kurzinfo CB-K21/0976 - Microsoft Windows Azure: Mehrere Schwachstellen
https://cert-bund.de/advisoryshort/CB-K21-0976

[BLE2021] OMIGOD: Microsoft Azure VMs exploited to drop Mirai, miners
https://www.bleepingcomputer.com/news/security/omigod-microsoft-azure-vms-exploited-to-drop-mirai-miners/

[MSR2021] Additional Guidance Regarding OMI Vulnerabilities within Azure VM Management Extensions
https://msrc-blog.microsoft.com/2021/09/16/additional-guidance-regarding-omi-vulnerabilities-within-azure-vm-management-extensions/

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.