Security Advisory 2021-051

Critical Vulnerabilities in Azure OMI Agents

September 15, 2021 — v1.0

TLP:WHITE

History:

- *15/09/2021 — v1.0 – Initial publication*

Summary

On 14th of September 2021, Microsoft released information about four vulnerabilities that affects Open Management Infrastructure (OMI) agent.

One vulnerability – CVE-2021-38647 [1] – is critical with CVSSv3 Score 9.8. If the HTTP/S port listening to OMI is exposed, it could allow remote code execution by sending a specially-crafted message from remote.

The other three vulnerabilities – CVE-2021-38645 [2], CVE-2021-38648 [3] and CVE-2021-38649 [4] – are related to privilege escalation that enables attackers to gain the `root` privileges on a machine with OMI installed.

The OMI agent is automatically deployed by certain Azure services. These parent services should handle the upgrade of the agents, however this has to be double checked. CERT-EU recommends to perform the upgrade as soon as possible.

Technical Details

CVE-2021-38647 [1] - OMI Remote Code Execution Vulnerability

Some Azure products, such as Azure Configuration Management or System Center Operations Manager (SCOM), expose an HTTP/S port listening to OMI requests. The configuration where the HTTP/S listener is enabled could allow remote code execution. It is important to mention that most Azure services that use OMI, deploy it without exposing the HTTP/S port. According to [6], any request without an authorization header has its privileges default to `uid=0`, `gid=0`, which is `root`.

CVE-2021-38645 [2], CVE-2021-38648 [3] and CVE-2021-38649[4] - OMI Elevation of Privilege Vulnerability

No technical details have been shared related to these vulnerabilities.

Products Affected

OMI agents version less than v1.6.8-1.

According to [6], the Linux machines built in Azure are at risk if they use any of the following services / tools:

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

In addition to Azure cloud, also the on-premise Linux machines with OMI installed as part of System Center (Microsoft's server management solution) for example, are also at risk.

Recommendations

Check if the OMI agent has the latest version as released in [5]. This can be done from Azure VMs by running the following commands in your terminal:

- for Debian systems (e.g., Ubuntu): `dpkg -l omi`
- for Redhat based system (e.g., Fedora, CentOS, RHEL): `rpm -qa omi`

If OMI is not installed, no results will be returned.

According to the security advisory [1], if the agent was not automatically installed, then the following steps should be taken:

- Add the MSRepo to your system. Based on the Linux OS that you are using, refer to this link [7] to install the MSRepo to your system.
- After that, use your platform's package tool to upgrade OMI (for example, `sudo apt-get install omi` or `sudo yum install omi`).

For more information refer to [8].

Workarounds and Mitigations

For CVE-2021-38647, check if you have the OMI listening ports open and limit access to them. For different services the port number could be different. On most Linux distributions, the command `netstat -an | grep <port-number>` will indicate if any processes are listening on `<port-number>`.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38645

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38648

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38649

[5] https://github.com/microsoft/omi-kits/tree/master/release

[6] https://www.wiz.io/blog/secret-agent-exposes-azure-customers-to-unauthorized-code-execution

[7] https://docs.microsoft.com/en-us/windows-server/administration/Linux-Package-Repository-for-Microsoft-Software

[8] https://github.com/microsoft/omi#get-omi