National Cyber Security Centre

2109171000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

OMI Vulnerabilities within Azure VM Management Extensions- CVE-2021-38645, CVE-2021-38649, CVE-2021-38648 & CVE-2021-38647 2021-09-17

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Four vulnerabilities exist in the Open Management Infrastructure (OMI) affecting many Linux Virtual Machines within Microsoft Azure. Three of these are Elevation of Privilege vulnerabilities and one is unauthenticated Remote Code Execution (RCE).

OMI is an open-source Web-Based Enterprise Management (WBEM) implementation for managing Linux and UNIX systems. Several Microsoft Virtual Machine (VM) management extensions use this framework to orchestrate configuration management and log collection on Linux VMs.

When Microsoft Azure customers set up a Linux Virtual Machine (VM) the OMI agent is automatically deployed when they enable certain Azure services. Unless a patch is applied, attackers can exploit these four vulnerabilities to escalate to root privileges and remotely execute malicious code. [1]

- CVE-2021-38647 – Unauthenticated RCE as root **(Severity: 9.8)**
- CVE-2021-38648 – Privilege Escalation vulnerability **(Severity: 7.8)**
- CVE-2021-38645 – Privilege Escalation vulnerability **(Severity: 7.8)**
- CVE-2021-38649 – Privilege Escalation vulnerability **(Severity: 7.0)**

Products Affected

Microsoft Azure servers which use certain VM Management Extensions with OMI versions below v1.6.8-1.

A full list of VM Management Extensions affected can be found here.

Impact

Remote Code Execution & Elevation of Privilege - compromised systems, data loss, privilege escalation.

Recommendations

Microsoft released a patched OMI version (1.6.8.1). In addition, Microsoft published mitigation guidance for the different impacted services. Customers may still be required to manually patch their machines. The NCSC recommends that affected organisations review the Microsoft Advisory.

To see if your Azure VMs may be vulnerable, you can run the commands below in your terminal to ensure OMI is updated to the latest version. If OMI is not installed you will get no results, if it is fully patched you will see it return Version 1.6.8.1:

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

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

DISCLAIMER: *This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie