UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00198

URGENT: OMIGOD CRITICAL VULNERABILITIES IN AZURE

DATE ISSUED: 16th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Four new critical vulnerabilities have been discovered in Microsoft Azure's implementation of Open Management Interface (OMI) and have been collectively dubbed "OMIGOD" affecting Linux Virtual Machines (VMs) which allow for Remote Code Execution (RCE) using a single request.

BREAKDOWN

Numerous Azure services are affected by the vulnerabilities, which are being tracked under CVE-2021-38647 (unauthenticated RCE as root), CVE-2021-38648, CVE-2021-38645, & CVE-2021-38649 (privilege escalation vulnerabilities) all carrying scores in the CVSS 9 range. Of a sample taken by Wiz researchers, 65% were affected and most are not aware they are at risk, as OMI's functions are largely undocumented with no clear guidelines around how to check or upgrade version. Some of the known impacted services include Azure Automation, Azure Automatic Update, Azure Operations Management Suite, Azure Log Analytics, Azure Configuration Management and Azure Diagnostics. Any user can communicate with OMI using a UNIX socket or an external use HTTP API and as OMI runs with root privileges attackers may be able to remotely access a machine, elevate privileges and execute arbitrary code and full takeover.

REMEDIATION STEPS

- Apply workarounds provided by Microsoft immediately and keep machines up to date with the latest versions. See references below. Check for released patches and solutions regularly.

REFERENCES & RESOURCES

Wiz	https://www.wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure
Dark Reading	https://www.darkreading.com/vulnerabilities-threats/omigod-azure-users-warned-of-critical-omi-vulnerabilities
ZDNet	https://www.zdnet.com/article/omigod-azure-users-running-linux-vms-need-to-update-now/
Rapid7	https://www.rapid7.com/blog/post/2021/09/15/omigod-how-to-automatically-detect-and-fix-microsoft-azures-new-omi-vulnerability/
Microsoft	https://docs.microsoft.com/en-us/windows-server/administration/Linux-Package-Repository-for-Microsoft-Software