OMIGOD: Microsoft Azure VMs exploited to drop Mirai, miners

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)**

September 17, 2021 11:23 AM **0**

Threat actors started actively exploiting the critical Azure OMIGOD (https://www.bleepingcomputer.com/tag/omigod/) vulnerabilities two days after Microsoft disclosed them during this month's Patch Tuesday.

The four security flaws (allowing privilege escalation and remote code execution) were found in the Open Management Infrastructure (OMI) software agent silently installed by Microsoft on more than half of all Azure instances.

In all, these bugs impact thousands of Azure customers and millions of endpoints, according to Wiz researchers Nir Ohfeld and Shir Tamari, who discovered them.

"With a single packet, an attacker can become root on a remote machine by simply removing the authentication header. It's that simple," Wiz researcher Nir Ohfeld said about the CVE-2021-38647 remote code execution (RCE) flaw.

"This vulnerability can be also used by attackers to obtain initial access to a target Azure environment and then move laterally within it."

Actively exploited to drop botnet and cryptomining malware

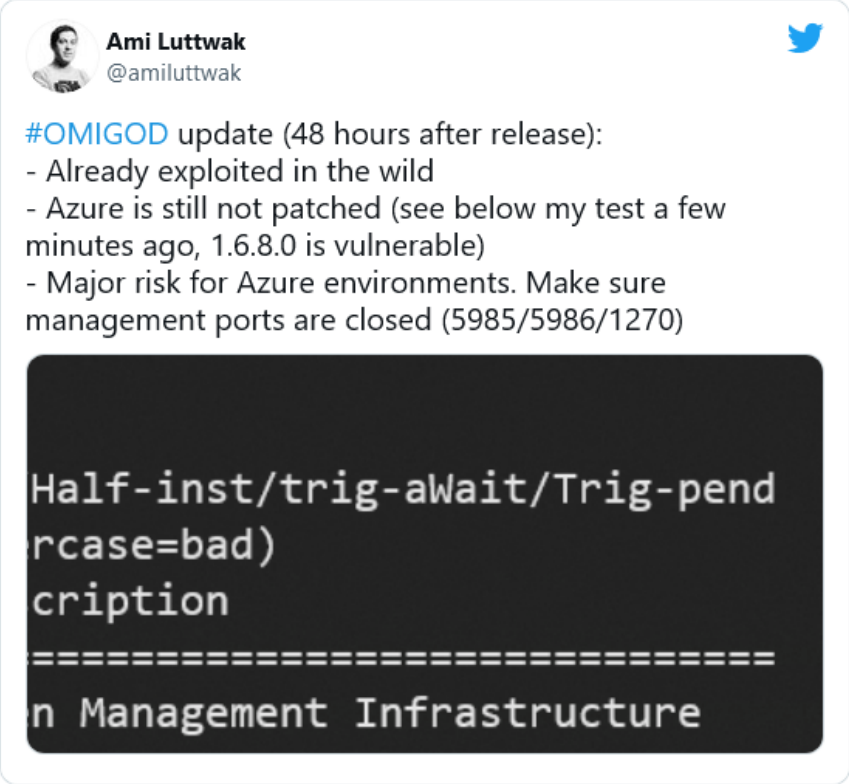
The first attacks were spotted yesterday evening by security researcher Germán Fernández (https://twitter.com/1ZRR4H/status/1438580885142507528) and were soon confirmed by cybersecurity companies GreyNoise (https://twitter.com/andrew____morris/status/1438598477718622214?s=12) and Bad Packets (https://twitter.com/bad_packets/status/1438753415106994179).

According to GreyNoise's current stats (https://www.greynoise.io/viz/query/?gnql=cve%3ACVE-2021-38647), attackers are scanning the Internet for exposed Azure Linux VMs vulnerable to CVE-2021-38647 exploits from over 110 servers.

A Mirai botnet is behind some of these exploitation attempts targeting Azure Linux OMI endpoints vulnerable to CVE-2021-38647 RCE exploits, as first spotted by Fernández (https://twitter.com/1ZRR4H/status/1438580885142507528) on Thursday evening.

Digital forensics firm Cado Security also analyzed the botnet malware (https://www.cadosecurity.com/azure-omi-vulnerability-omigod-cve-2021-38647-now-under-exploitation/) dropped on compromised systems and found that it also "closes the ports of the vulnerabilities it exploited to stop other botnets taking over the system."

As security researcher Kevin Beaumont found (https://twitter.com/GossiTheDog/status/1438604418212114440), other threat actors are targeting OMIGOD-vulnerable Azure systems to deploy cryptominer payloads.



(https://twitter.com/amiluttwak/status/1438640680763633665)

How to secure your Azure VM

While Microsoft has released patched a patched OMI software agent version (https://github.com/microsoft/omi/releases) more than a week ago, the company is still in the process of rolling out security updates to cloud customers who have automatic updates enabled in their VMs.

According to additional guidance Redmond released today, "customers must update vulnerable extensions for their Cloud and On-Premises deployments as the updates become available" per a predefined schedule (https://www.bleepingcomputer.com/news/microsoft/microsoft-asks-azure-linux-admins-to-manually-patch-omigod-bugs/) shared by the Microsoft Security Response Center team.

"New VMs in these regions will be protected from these vulnerabilities post the availability of updated extensions."

To manually update the OMI agent on your VM, you can also use the built-in Linux package manager:

- Add the MSRepo to your system. Based on the Linux OS that you are using, refer to this link to install the MSRepo to your system: Linux Software Repository for Microsoft Products | Microsoft Docs (https://docs.microsoft.com/en-us/windows-server/administration/Linux-Package-Repository-for-Microsoft-Software)
- You can then use your platform's package tool to upgrade OMI (for example, `sudo apt-get install omi` or `sudo yum install omi`).

"While updates are being rolled out using safe deployment practices, customers can protect against the RCE vulnerability by ensuring VMs are deployed within a Network Security Group (NSG) or behind a perimeter firewall and restrict access to Linux systems that expose the OMI ports (TCP 5985, 5986, and 1207)," Microsoft added.