Hive Pro

THREAT ADVISORY

Threat actors are actively exploiting OMIGOD vulnerabilities impacting Microsoft Azure

TA202135

Threat Level AMBER

Publish Date – September 19, 2021

Azure VMs using Linux management solutions with Azure Automation, Azure Automatic Update, Azure Operations Management Suite (OMS), Azure Log Analytics, Azure Configuration Management, or Azure Diagnostics are affected by OMIGOD. Attackers can remotely exploit a vulnerable piece of management software in the Open Management Infrastructure (OMI) architecture, allowing them to elevate to root access and execute malicious code. Microsoft is not automatically updating insecure agents, Hive pro threat research advises users to update to the latest version manually.

Vulnerability Details

CVE ID	Affected CPEs	Vulnerability Name
CVE-2021-38647	cpe:2.3:a:microsoft:azure_open_management_infrastructure:*:*:*:*:*:*:*:*	Unauthenticated RCE as root
CVE-2021-38648		Privilege Escalation vulnerability
CVE-2021-38645		
CVE-2021-38649		

Indicators of Compromise

Type	Value
IPV4	212.192.241[.]72
Hash(SHA1)	034d4d30c8c4777bf3531c78839f947cf41682784f8f80567c0fed5a49ac362f, 15b2a15ed77a3b4ac4f0ed53f607265c8b892ed1f20a8258a936a4948a7486a2, 4976c1cfa9471fc568075ef75a7271de87fb40811ef0ef89a49e112b05acc61a, 4e40678485aa14f4e213362043aadd1e78f0f43bb4dffef6454ec2c4104074fb, 594e4c06ba7c9b5b588efc6526d5ae67c59a2969967bd0b700741561fc069faf, 81cc484036eeb43dae1a7d10f3222854aba9e549bd4b0c8b61b4700da03d65e6, 85a2c4b2701b05abd430adcd761d9a433dca04dbf7b27ee53f629c3aa86b5117, 8ecc0d9f044fd28f6a0df24e2f8220d293150029b9504aecca3d13eea007573d, 9338416ba46e59a2db1ef0f11189c6fae73275ee8675cf4d7487e08d98d1968f 9c658f2f8b92a7cf44b06602c257ffeefb934e4b9432d675deb129518a4b7d76, a71ef3277ddaa731310cd810ff919d480a402688c725fefd3fd8792f5552f94a, ccf73ee5dfecc4bc7545a5ad51626ac3b1a847ccd73a768710ca9d8396a4845e, d3f7db6fb50a3d050cb6560d890ec06cd0d94b7f75364fa9b255909704cfdd35, d999589d8002f8d91f3fd3148f33da441f5a3a814c71180dba685fe89864dac6, e04300d699568deba0b1ebaf94059aebd4e6b6222e01e31347373e139aef4fee, e9881d1222e959ea5f95a045a11835d06c32b0e0bee44136cabf1fc78b99f8d3, f1fd17e5a355d9885982c7f2eafe236efd73dd29d048f95b22e0caf9e044131b, f66c817439d7286b54d2f193162c2d665bbca489dbae4926edbc821446d366b2, fb09d0036ca129907851617e8aa831e0615b2de0dab4f2836598fa97f8c4d187, fe2cb1e1530cc94e1faf23a50bb7c5f4a81c80f14eaf0a3a28251cf6f76ca09e

Patch Links

https://msrc-blog.microsoft.com/2021/09/16/additional-guidance-regarding-omi-vulnerabilities-within-azure-vm-management-extensions/

References

https://www.bleepingcomputer.com/news/security/omigod-microsoft-azure-vms-exploited-to-drop-mirai-miners/
https://msrc-blog.microsoft.com/2021/09/16/additional-guidance-regarding-omi-vulnerabilities-within-azure-vm-management-extensions/