



THREAT ADVISORY

**ATTACK
REPORT**

Monti ransomware infiltrates networks via the well-known Log4Shell

Date of Publication

September 14, 2022

Admiralty Code

A1


TA Number

TA2022202

Summary

The Monti ransomware infiltrated the client's internet-facing VMware Horizon virtualization system by exploiting the well-known "Log4Shell" vulnerability, a.k.a. CVE-2021-44228. Furthermore, the threat actor employed a commercial, cloud-based remote monitoring and maintenance (RMM) platform named Action1, which has never been used in a ransomware campaign before.

⚙️ CVE Table

CVE	NAME	PATCH
CVE-2021-44228	Apache Log4j Remote Code Execution Vulnerability	

🔗 Potential MITRE ATT&CK TTPs

TA0001 Initial Access	T1190 Exploit Public-Facing Application	TA0008 Lateral Movement	T1210 Exploitation of Remote Services
TA0002 Execution	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	TA0040 Impact
T1496 Resource Hijacking	T1486 Data Encrypted for Impact	TA0005 Defense Evasion	T1140 Deobfuscate/Decode Files or Information
T1553 Subvert Trust Controls	T1036 Masquerading	T1036.001 Invalid Code Signature	T1055 Process Injection
TA0003 Persistence	T1505 Server Software Component	TA0004 Privilege Escalation	T1068 Exploitation for Privilege Escalation

Technical Details

#1

The attackers used two well-known temporary file transfer websites, dropmefiles.com[.]ua and temp[.]sh, to bring tools into the network and exfiltrate data. They utilized the Google Chrome web browser to access these sites and download tools.

#2

The ransomware payload dropped after the initial infection was a 32-bit Windows executable named "locker.exe." Upon execution, the ransomware encrypts files on disc, adds a ".PUUUK" extension to encrypted file names, and produces the ransom note.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2021-44228	VMware Horizon 8.0, 7.0	cpe:2.3:a:vmware:horizon:*:*:*:*:*:*	CWE-917 CWE-502 CWE-400 CWE-20

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	b45fe91d2e2340939781d39daf606622e6d0b9ddacd8425cb8e49c56124c1d56, 158dcb26239a5db7a0eb67826178f1eaa0852d9d86e59afb86f04e88096a19bc, 702099b63cb2384e11f088d6bc33afbd43a4c91848f393581242a6a17f1b30a0, 9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cb e732, df492b4cc7f644ad3e795155926d1fc8ece7327c0c5c8ea45561f24f5110ce54, 78517fb07ee5292da627c234b26b555413a459f8d7a9641e4a9fcc1099f06a3d

Patch Links

<https://www.vmware.com/security/advisories/VMSA-2021-0028.html>

References

<https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger>

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 14, 2022 • 5:49 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com