Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Chinese Espionage Hackers Exploit ESXi Zero-Day

Date of Publication	Admiralty Code	TA Number
June 14, 2023	A2	TA2023263

Summary

First appeared: September 2022
Actor Name: UNC3886
Malware: VirtualPita and VirtualPie backdoors
Attack Region: The US and APJ regions.
Targeted Sectors: Defense, Technology, and Telecommunication.
Targeted Platforms: Windows, Linux, and PhotonOS (vCenter) guest VMs
Attack: The Chinese-sponsored hacking group, UNC3886, has been actively exploiting the CVE-2023-20867 vulnerability and using advanced backdoors such as VirtualPita and VirtualPie to carry out malicious activities across organizations in the US and APJ regions.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-20867	VMware Tools authentication bypass	VMware Tools: 10.0.0 - 12.2.0	✓	✗	✓

Attack Details

#1 The Chinese-sponsored hacking group UNC3886 utilized a zero-day vulnerability (CVE-2023-20867) in VMware ESXi to exploit an authentication bypass flaw within VMware Tools. This enabled them to Stealthily deploy VirtualPita and VirtualPie backdoors on both Windows and Linux systems, including guest VMs, originating from compromised ESXi hosts.

#2 The primary objective of this nefarious activity was to illicitly acquire sensitive data. In the event of a fully compromised ESXi host, the manipulation of VMware Tools can fail to authenticate host-to-guest operations, thereby compromising the confidentiality and integrity of the guest virtual machine. UNC3886 has predominantly targeted defense, technology, and telecommunication organizations located in the United States and APJ (Asia Pacific and Japan) regions.

#3 In the subsequent phase, UNC3886 deployed VirtualPita and VirtualPie backdoors into ESXi and vCenter machines, ensuring the concealment of their malicious operations. Notably, UNC3886 has demonstrated the deployment of multiple backdoors, such as VIRTUALGATE and VIRTUALPITA, using VMCI sockets to facilitate lateral movement and maintain a persistent presence within the compromised infrastructure.

#4 When an ESXi host is initially connected to a vCenter server, a service account called 'vpxuser' is created. UNC3886 has been observed harvesting the credentials of this vpxuser account from vCenter servers, thereby acquiring administrative privileges over all associated ESXi hosts. By exploiting the CVE-2023-20867 vulnerability, the threat actor can execute privileged commands across guest virtual machines, leveraging the harvested credentials of the connected ESXi service accounts from the vCenter Server appliance.

#5 UNC3886 persistently focuses on devices and platforms that typically lack EDR (Endpoint Detection and Response) solutions, effectively leveraging zero-day exploits on these specific platforms. During their mid-2022 campaign, the Chinese hacking group UNC3886 exploited a zero-day vulnerability (CVE-2022-41328) to compromise FortiGate firewall devices and successfully deploy previously undiscovered Castletap and Thincrust backdoors.

Recommendations

Ensuring Regular Patching and Vulnerability Management: Organizations must prioritize timely patching and updates for their virtualization platforms, such as VMware ESXi and vCenter, to effectively address known vulnerabilities. By promptly applying patches and keeping systems up-to-date through the upgrade to VMware Tools version 12.2.5 or later, the risk of exploitation can be significantly reduced, effectively thwarting potential attacks from threat actors like UNC3886.

Implement Least Privilege and Access Controls: Organizations must adopt strong access controls, employing least privilege principles. This involves restricting administrative access to authorized personnel, implementing multifactor authentication, enforcing regular password updates, limiting the use of service accounts, and regularly reviewing access privileges. These measures mitigate the risk of unauthorized access and credential abuse highlighted by UNC3886's exploitation of administrative privileges and credential harvesting.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control	T1560 Archive Collected Data
T1059 Command and Scripting Interpreter	T1203 Exploitation for Client Execution	T1569 System Services	T1098 Account Manipulation
T1136 Create Account	T1543 Create or Modify System Process	T1548 Abuse Elevation Control Mechanism	T1068 Exploitation for Privilege Escalation
T1055 Process Injection	T1211 Exploitation for Defense Evasion	T1212 Exploitation for Credential Access	T1087 Account Discovery
T1105 Ingress Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	8e80b40b1298f022c7f3a96599806c43 2c28ec2d541f555b2838099ca849f965 744e2a4c1da48869776827d461c2b2ec 93d50025b81d3dbcb2e25d15cae03428 fe34b7c071d96dac498b72a4a07cb246 61ab3f6401d60ec36cd3ac980a8deb75
SHA1	e9cbac1f64587ce1dc5b92cde9637affb3b58577 e35733db8061b57b8fcdb83ab51a90d0a8ba618c a3cc666e0764e856e65275bd4f32a56d76e51420 abff003edf67e77667f56bbcfc391e2175cb0f8a 0962e10dc34256c6b31509a5ced498f8f6a3d6b6 93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84
SHA256	c2ef08af063f6d416233a4b2b2e991c177fc72d70a76c24bca9080521d41040f,505eb3b90cd107cf7e2c20189889afdff813b2fbb98bbdeab65cde520893b168,4a6f559426493abc0d056665f23457e2779abd3482434623e1f61f4cd5b41843,13f11c81331bdce711139f985e6c525915a72dc5443fbbfe99c8ec1dd7ad2209,5731d988781c9a1d2941f7333615f6292fb359f6d48498f32c29878b5bedf00f,4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b264ae0d1e15e70d

Patch Links

https://www.vmware.com/security/advisories/VMSA-2023-0013.html

References

https://www.mandiant.com/resources/blog/vmware-esxi-zero-day-bypass

https://core.vmware.com/vsphere-esxi-mandiant-malware-persistence#introduction

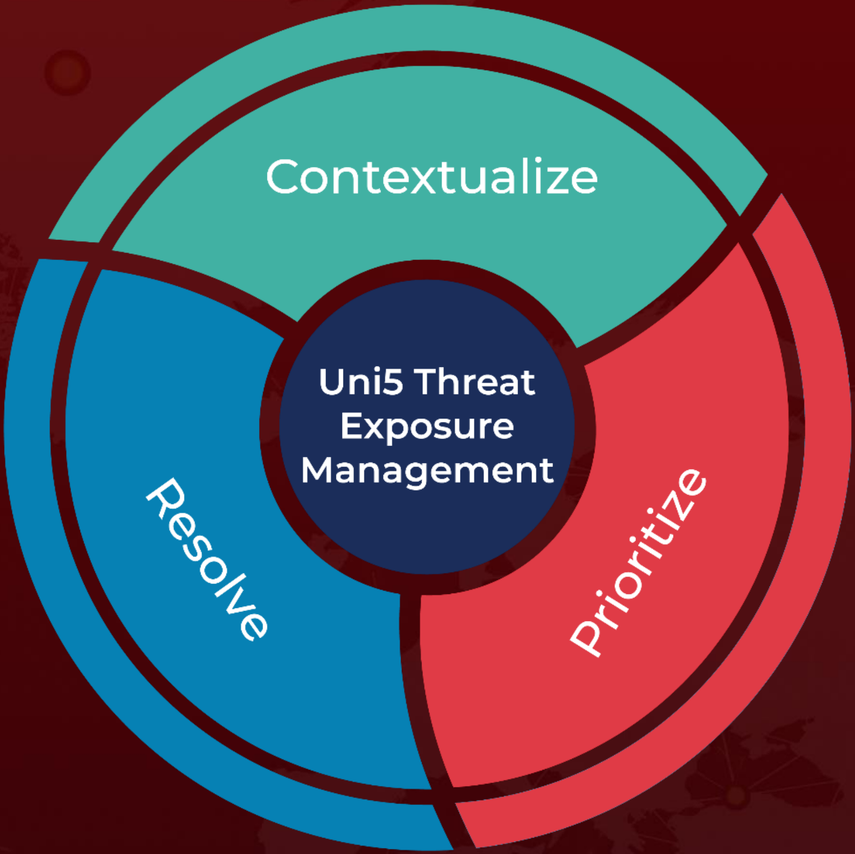
https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence

https://www.hivepro.com/unc3886-targets-technologies-with-custom-malware-and-exploits-zero-day-vulnerabilities/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 14, 2023 • 8:59 AM

More at www.hivepro.com