Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Cybercrime group exploits zero-day on Windows servers to deploy Nokoyawa ransomware

Date of Publication

April 12, 2023

Admiralty Code

A1

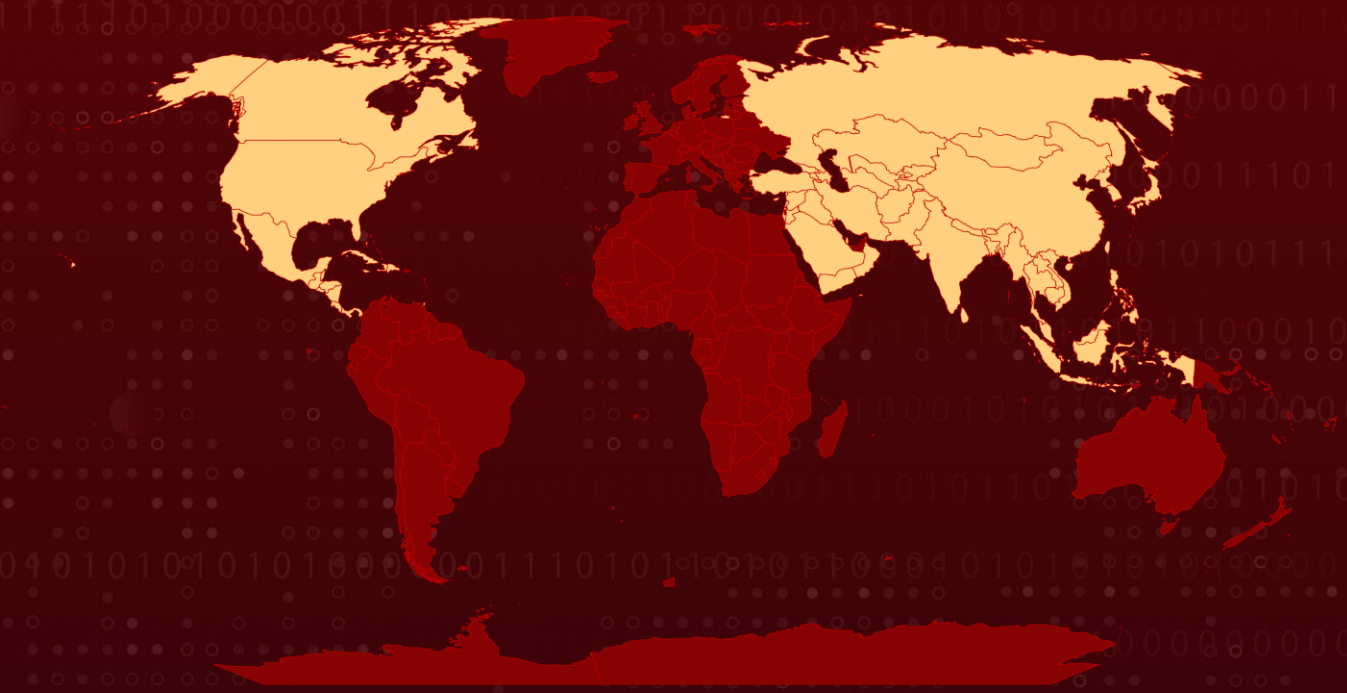
TA Number

TA2023180

Summary

First Appearance: February 2022
Targeted Countries: North America, Middle East, and Asia.
Malware: Nokoyawa ransomware
Targeted Industries: Healthcare, Manufacturing, Energy, Wholesale, Retail
Affected Platforms: Windows
Attack: Nokoyawa ransomware is a new threat that exploits the CVE-2023-28252 vulnerability to infiltrate and encrypt victims' files, demanding a ransom for their release.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	PATCH	Zero-day	CISA KEV
CVE-2023-28252	Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	✓	✓	✓

Attack Details

#1

A zero-day vulnerability, CVE-2023-28252, in the Common Log File System (CLFS) driver, which is a log file subsystem implemented in the clfs.sys driver of Microsoft Windows servers. A cybercrime group, notable for its use of a large number of similar but unique CLFS driver exploits that were likely developed by the same exploit author, attempted to deploy Nokoyawa ransomware as a final payload using this zero-day.

#2

The exploit is an out-of-bounds write (increment) vulnerability that can be exploited when the system attempts to extend the metadata block. The discovered exploit uses the vulnerability to corrupt another specially crafted base log file object in a way that a fake element of the base log file gets treated as a real one. The attacker must be authenticated with user access and have the ability to run code on the target system to launch the elevation-of-privilege exploit. Microsoft has patched this vulnerability as part of April Patch Tuesday.

Recommendations

To protect against this vulnerability and potential attacks, it is recommended that all Microsoft Windows servers be updated immediately with the latest security patches.

Organizations should ensure that all user accounts have appropriate access levels and permissions to limit the potential impact of a successful attack. It is also important to regularly monitor system logs and network activity for any suspicious behavior. Regularly backing up data can also aid in recovery from a ransomware attack.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
T1218.001 Compiled HTML File	T1106 Native API	T1082 System Information Discovery	T1027 Obfuscated Files or Information
T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter	T1218 System Binary Proxy Execution	T1069.002 Domain Groups
T1127 Trusted Developer Utilities Proxy Execution	T1127.001 MSBuild	T1068 Exploitation for Privilege Escalation	T1176 Browser Extensions
T1190 Exploit Public-Facing Application	T1564 Hide Artifacts	T1574 Hijack Execution Flow	T1486 Data Encrypted for Impact
T1543 Create or Modify System Process			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	46168ed7dbe33ffc4179974f8bf401aa 1e4dd35b16ddc59c1ecf240c22b8a4c4 f23be19024fcc7c8f885dfa16634e6e7 A2313d7fdb2f8f5e5c1962e22b504a17 8800e6f1501f69a0a04ce709e9fa251c
Domains	vnssinc[.]com qooqle[.]top vsexec[.]com devsetgroup[.]com

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252

References

https://securelist.com/nokoyawa-ransomware-attacks-with-windows-zero-day/109483/

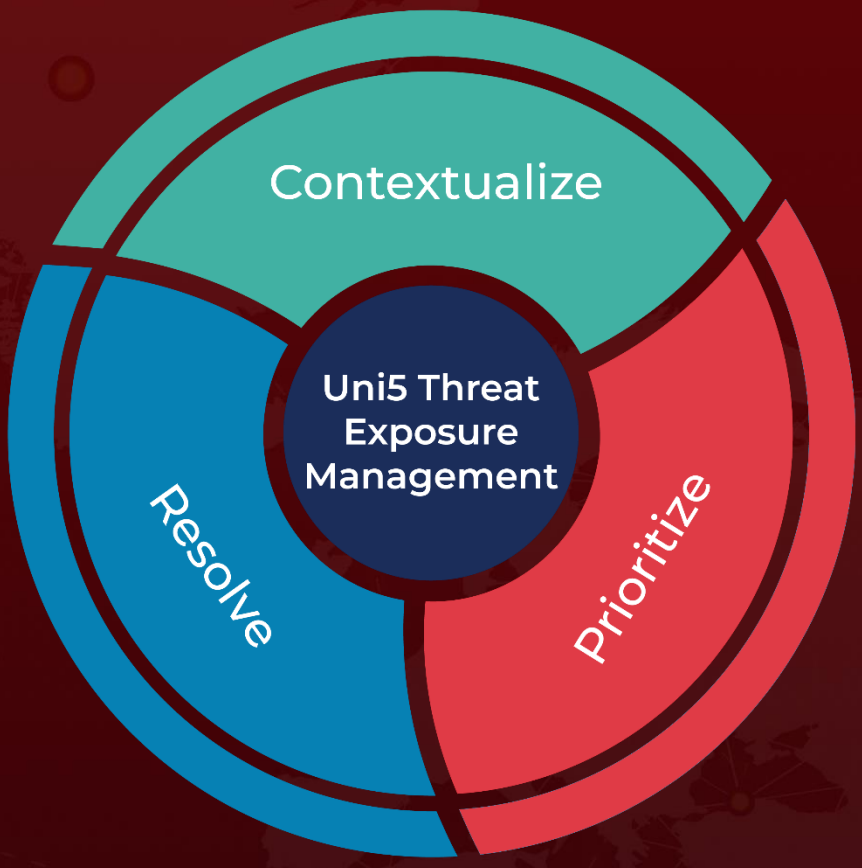
https://www.kaspersky.com/about/press-releases/2023_zero-day-in-microsoft-windows-used-in-nokoyawa-ransomware-attacks

https://www.hivepro.com/nokoyawa-2-0-a-reworked-rust-based-ransomware/

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

April 12, 2023 • 1:30 AM

More at www.hivepro.com