Hive Pro

THREAT ADVISORY

Have you patched the vulnerabilities in Microsoft Exchange Server?	TA202130
Threat Level RED	**Publish Date –** Aug 18, 2021

Microsoft Exchange Server vulnerabilities have been officially patched for five months now. These vulnerabilities are actively exploited by multiple threat actors named DeadRinger. DeadRinger has been affecting the telecommunication industry all around the world. DeadRinger consists of three clusters. The first one includes threat group Softcell which has been active since 2012. The Naikon group, which has been active since 2020, is the second cluster. We discovered that the signatures match those of TG-3390, making it the third cluster.
As a response, Hive Pro Threat Researchers advises that you address these vulnerabilities.

The Techniques used by the DeadRinger includes:
T1592: Gather Victim Host Information
T1595: Active Scanning
T1590: Gather Victim Network Information
T1190: Exploit Public-Facing Application
T1059: Command and Scripting Interpreter
T1047: Windows Management Instrumentation
T1059.001: Command and Scripting Interpreter: PowerShell
T1505.003: Server Software Component: Web Shell
T1136: Create Account
T1053: Scheduled Task/Job
T1078: Valid Accounts
T1574: Hijack Execution Flow
T1027.005: Obfuscated Files or Information: Indicator Removal from Tools
T1027: Obfuscated Files or Information
T1036: Masquerading
T1070.006: Indicator Removal on Host: Timestomp
T1140: Deobfuscate/Decode Files or Information
T1040: Network Sniffing
T1087: Account Discovery
T1018: Remote System Discovery
T1071.001: Application Layer Protocol: Web Protocols
T1041: Exfiltration Over C2 Channel
T1021.002: Remote Services: SMB/Windows Admin Shares
T1550.002: Use Alternate Authentication Material: Pass the Hash
T1105: Ingress Tool Transfer

T1555: Credentials from Password Stores
T1003: OS Credential Dumping
T1016: System Network Configuration Discovery
T1069: Permission Groups Discovery
T1560: Archive Collected Data
T1569: System Services
T1543.003: Create or Modify System Process: Windows Service
T1574.002: Hijack Execution Flow: DLL Side-Loading
T1570: Lateral Tool Transfer
T1056.001: Input Capture: Keylogging
T1573: Encrypted Channel

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Name
CVE-2021-26855	Microsoft Exchange Server 2013, Microsoft Exchange Server 2016, Microsoft Exchange Server 2019	cpe:2.3:a:microsoft:exchange_server:2013_cu23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu18:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu19:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu7:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu8:*:*:*:*:*:*:*	SSRF vulnerability in Microsoft Exchange Server
CVE-2021-26857			An insecure deserialization vulnerability in Microsoft Exchange
CVE-2021-26858			An arbitrary file write vulnerabilities in Microsoft Exchange
CVE-2021-27065			An arbitrary file write vulnerabilities in Microsoft Exchange

Actor Details

Name	Known as	Origin	Target Locations	Target sectors
Soft Cell	Gallium , PHANTOM PANDA	China	Worldwide	Telecommunications.
Naikon	Hellsing, Lotus Panda,ITG06	China	Australia, Brunei, Cambodia, China, India, Indonesia, Laos, Malaysia, Myanmar, Nepal, Philippines, Saudi Arabia, Singapore, South Korea, Thailand, USA, Vietnam.	Defense, Energy, Government, Law enforcement, Media, Telecommunications.
Emissary Panda	APT 27 ,LuckyMouse, Bronze Union,TG-3390, TEMP.Hippo ,Budworm,Group 35 ,ATK 15 ,Iron Tiger ,Earth Smilodon ,ZipToken	China	Australia, Canada, China, Hong Kong, India, Iran, Israel, Japan, Mongolia, Philippines, Russia, Spain, South Korea, Taiwan, Thailand, Tibet, Turkey, UK, USA and Middle East.	Aerospace, Aviation, Defense, Education, Embassies, Government, Manufacturing, Technology, Telecommunications, Think Tanks.

Indicators of Compromise (IoCs)

Type	Value
IP Address	47.56.86[.]44 45.76.213[.]2 45.123.118[.]232 101.132.251[.]212
SHA-1 Hash	19e961e2642e87deb2db6ca8fc2342f4b688a45c ba8f2843e2fb5274394b3c81abc3c2202d9ba592 243cd77cfa03f58f6e6568e011e1d6d85969a3a2 c549a16aaa9901c652b7bc576e980ec2a008a2e0 c2850993bffc8330cff3cb89e9c7652b8819f57f 440e04d0cc5e842c94793baf31e0d188511f0ace e2340b27a4b759e0e2842bfe5aa48dda7450af4c 15336340db8b73bf73a17c227eb0c59b5a4dece2 5bc5dbe3a2ffd5ed1cd9f0c562564c8b72ae2055 0dc49c5438a5d80ef31df4a4ccaab92685da3fc6 81cfcf3f8213bce4ca6a460e1db9e7dd1474ba52 e93ceb7938120a87c6c69434a6815f0da42ab7f2 207b7cf5db59d70d4789cb91194c732bcd1cfb4b 71999e468252b7458e06f76b5c746a4f4b3aaa58 39c5c45dbec92fa99ad37c4bab09164325dbeea0 efc6c117ecc6253ed7400c53b2e148d5e4068636 a3c5c0e93f6925846fab5f3c69094d8a465828e9 a4232973418ee44713e59e0eae2381a42db5f54c 5602bf8710b1521f6284685d835d5d1df0679b0f e3fcda85f5f42a2bffb65f3b8deeb523f8db2302 720556854fb4bcf83b9ceb9515fbe3f5cb182dd5 b699861850e4e6fde73dfbdb761645e2270f9c9a 6516d73f8d4dba83ca8c0330d3f180c0830af6a0 99f8263808c7e737667a73a606cbb8bf0d6f0980 a5b193118960184fe3aa3b1ea7d8fd1c00423ed6 92ce6af826d2fb8a03d6de7d8aa930b4f94bc2db d9e828fb891f033656a0797f5fc6d276fbc9748f 87c3dc2ae65dcd818c12c1a4e4368f05719dc036
Domain	Cymkpuadkduz[.]xyz nw.eiyfmrn[.]com jdk.gsvvfsso[.]com ttareyice.jkub[.]com my.eiyfmrn[.]com A.jrmfeeder[.]org afhkl.dseqoorg[.]com

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26857
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26858
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27065

References

https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
https://www.zdnet.com/article/deadringer-chinese-apts-strike-major-telecommunications-companies/