Hive Pro

THREAT ADVISORY

BlackByte ransomware exploits Microsoft Servers ProxyShell vulnerabilities	TA202155
Threat Level RED	**Publish Date –** Dec 7, 2021

BlackByte ransomware is targeting organizations with unpatched ProxyShell vulnerabilities. Proxy Shell was addressed by hive pro threat researcher in the previous advisory released on August 24.

ProxyShell is a combination of three flaws in Microsoft Exchange:

CVE-2021-34473 Pre-auth path confusion vulnerability to bypass access control.
CVE-2021-34523 Privilege escalation vulnerability in the Exchange PowerShell backend.
CVE-2021-31207 Post-auth remote code execution via arbitrary file write.

These security flaws are used together by threat actors to perform unauthenticated, remote code execution on vulnerable servers. After exploiting these vulnerabilities, the threat actors then installs web shells, coin miners, ransomwares or backdoors on the servers. Attackers then use this web shell to deploy cobalt strike beacon into Windows Update Agent and get the credentials for a service account on compromised servers. The actor then installs Anydesk to gain control of the system and do lateral movement in the organization network. Post exploitation, attackers carry on with using Cobalt Strike to execute the Blackbyte ransomware and encrypt the data.

Affected organizations can decrypt their files using a free decryption tool written by Trustwave. Users can patch their server for ProxyShell vulnerabilities using the link down below.

Techniques used by Blackbyte ransomware are :
T1505.003 Server Software Component: Web Shell
T1055 Process Injection
T1059.001 Command and Scripting Interpreter: PowerShell
T1595.002 Active Scanning: Vulnerability Scanning
T1027 Obfuscated Files of Information
T1490 Inhibit System Recovery
T1112 Modify Registry
T1562.001 Impair Defenses: Disable or Modify Tools
T1562.004 Impair Defenses: Disable or Modify System Firewall
T1018 Remote System Discovery
T1016 System Network Configuration Discovery
T1070.004 Indicator Removal on Host: File Deletion
T1560.001 Archive Collected Data: Archive via Utility

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Name
CVE-2021-34473	Microsoft Exchange Server 2013 CU23, 2016 CU19, 2016 CU20, 2019 CU8, 2019 CU9	cpe:2.3:a:microsoft:exchange_server:2013_cu23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu19:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu20:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu8:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu9:*:*:*:*:*:*:*	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-34523			Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2021-31207			Microsoft Exchange Server Security Feature Bypass Vulnerability

Actor Details

Name	Target Locations	Target sectors
BlackByte Ransomware	USA, Australia, France, Italy, Chile, Turkey, and Croatia.	manufacturing, food, beverage, mining, construction, and healthcare

Indicators of Compromise (IoCs)

Type	Value
IP Address	185.93.6.31
SHA-2 Hash	829751cfdc2376e916244f94baf839ce4491ccb75f0a89778c092bde79bd8643 1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad 91f8592c7e8a3091273f0ccbfe34b2586c5998f7de63130050cb8ed36b4eec3e

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31207

References

https://redcanary.com/blog/blackbyte-ransomware/
https://www.techtarget.com/searchsecurity/news/252510334/BlackByte-ransomware-attacks-exploiting-ProxyShell-flaws
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-blackbyte-ransomware/
https://www.stellarinfo.com/blog/blackbyte-ransomware-attacks-exchange-servers-with-proxyshell-flaws/