Hive Pro

THREAT ADVISORY

MuddyWater is taking advantage of old vulnerabilities.

TA202149

Threat Level RED

Publish Date – Nov 18, 2021

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC) have issued a joint advisory to warn organizations about an APT State-sponsored Actor exploiting old Fortinet and proxyshell vulnerabilities.

Since late March 2021, this APT Iranian State-sponsored Actor (MuddyWater) has been breaching vulnerable networks by exploiting Fortinet vulnerabilities. The Hive Pro threat Research team has issued a detailed and in - depth advisory for the same.

Now, in October 2021, MuddyWater is getting initial access to the susceptible system by exploiting the well-known ProxyShell Vulnerability (CVE-2021-34473).
It is recommended that organizations patch these vulnerabilities as soon as available.

The **Tactics** and **Techniques** used by MuddyWater are:
TA0042 - Resource Development
T1588.001 - Obtain Capabilities: Malware
T1588.002 - Obtain Capabilities: Tool
TA0001 - Initial Access
T1190 - Exploit Public- Facing Application
TA0002 - Execution
T1053.005 - Scheduled Task/Job: Scheduled Task
TA0003 - Persistence
T1136.001 - Create Account: Local Account
T1136.002 - Create Account: Domain Account
TA0004 - Privilege Escalation
TA0006 - Credential Access
TA0009 - Collection
T1560.001 - Archive Collected Data: Archive via Utility
TA0010 - Exfiltration
TA0040 - Impact
T1486 - Data Encrypted for Impact

Actor Details

Name	Known As	Origin	Target Location	Target Sector
MuddyWater	Seedworm, TEMP.Zagros, Static Kitten, NTSTATS, POWERSTATS, MERCURY	IRAN	Armenia, Azerbaijan, Georgia, Germany, Iraq, Jordan, Malta, Netherlands, Pakistan, Tajikistan, Saudi Arabia, Turkey, Turkmenistan, United Arab Emirates	Defense, Education, Food, Gaming, Government, IT, Media, NGOs, Oil and gas, Telecommunications, Academic, Transportation

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-34473	Microsoft Exchange Server 2013 CU23, 2016 CU19, 2016 CU20, 2019 CU8, 2019 CU9	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*	Microsoft Exchange Server Remote Code Execution Vulnerability	
CVE-2018-13379	5.4.6 to 5.4.12, 5.6.3 to 5.6.7, 6.0.0 to 6.0.4	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	A path traversal vulnerability in the FortiOS SSL VPN web portal	CWE-22
CVE-2019-5591	6.2.0		Lack of LDAP server identity verification in default configuration	CWE-200
CVE-2020-12812	6.4.0, 6.2.0 to 6.2.3, 6.0.9		FortiOS SSL VPN 2FA bypass	CWE-287

Indicators of Compromise(IoCs)

Type	Value
IP Addresses	91.214.124[.]143 162.55.137[.]20 154.16.192[.]70
SHA1 Hash	95E045446EFB8C9983EBFD85E39B4BE5D92C7A2A A8674983A45BD88A4D11BCFD686C2BF8182831A0 F1D90E10E6E3654654E0A677763C9767C913F8F0 CDCD97F946B78831A9B88B0A5CD785288DC603C1 5BD0690247DC1E446916800AF169270F100D089B C4160AA55D092CF916A98F3B3EE8B940F2755053
MD5 Hash	E64064F76E59DEA46A0768993697EF2F

Patch Link

https://kb.fortinet.com/kb/documentLink.do?externalID=FD37033
http://www.securityfocus.com/bid/108693
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473

References

https://us-cert.cisa.gov/ncas/alerts/aa21-321a