Hive Pro

THREAT DIGEST

Fix What Matters to Your Business

Summary of Vulnerabilities & Threats

24-30 October 2022

The last week of October 2022 witnessed the discovery of 375 vulnerabilities out of which eight gained the attention of security researchers worldwide. Among these eight, one vulnerability is awaiting re-analysis on the NVD. Hive Pro Threat Research Team advises organizations to patch this vulnerability as soon as possible.

A critical issue in OpenSSL that could be remotely exploited to compromise server private keys or run code is yet to acquire a security update this week. This week also witnessed the most recent LV ransomware infiltration involved the intrusion of a Jordan- based entity's corporate environment by exploiting ProxyShell weaknesses to extort data.

Further, we also observed five Threat Actor groups being highly active in the last week. First was the Daixin Team, an unknown threat actor, popular for financial gain. The second was the SideWinder, an Indian threat actor group, popular for Information theft and espionage leveraged campaigns against government and business sectors throughout Asia. The third was the Lazarus Group, a North Korean threat actor popular for a financial crime that exploited known vulnerabilities within Dream Security's MagicLine4NX. The threat actors Hafnium and OilRig coordinated a massive effort to exploit Fortinet vulnerabilities. Common TTPs which could potentially be exploited by these threat actors or CVEs can be found in the detailed section.

Published Vulnerabilities	Interesting Vulnerabilities	Active Threat Groups	Targeted Countries	Targeted Industries	ATT&CK TTPs
375	8	5	55	13	44

Detailed Report

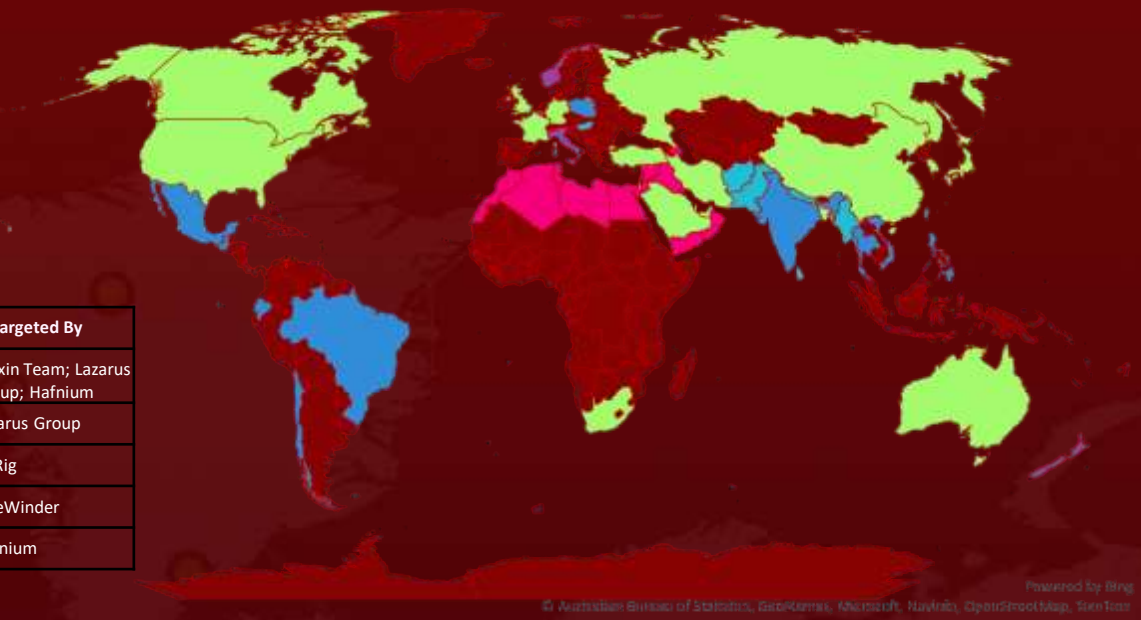
Interesting Vulnerabilities

VENDOR	CVE	PATCH LINK
DREAM SECURITY Digital Trust	CVE-2021-26606	UpdateMagicLine4.0 to version 1.0.0.18 or later Patch Link: http://demo.initech.com/initech/crosswebex_pack/3.3.2.36/INIS_EX_SHA2_3.3.2.36.exe
SQLite	CVE-2022-35737	https://www.sqlite.org/cves.html
vmware	CVE-2021-39144 CVE-2022-31678	https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4.14/rn/vmware-nsx-data-center-for-vsphere-6414-release-notes/index.html https://kb.vmware.com/s/article/89809
FORTINET	CVE-2022-40684	Upgrade to FortiOS version 7.07 or 7.2.2 or above Upgrade to FortiProxy version 7.07 or 7.2.1 or above Upgrade to FortiSwitchManager version 7.2.1 or above
Microsoft	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	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

Active Actors

ICON	NAME	ORIGIN	MOTIVE
	Daixin Team	Unknown	Financial gain
	SideWinder (Rattlesnake,T-APT-04,APT-C-17, Razor Tiger, Baby Elephant , Operation Origami)	India	Information theft and espionage
	Lazarus Group (Labyrinth Chollima, Group 77, HastatiGroup, WhoisHacking Team, NewRomanicCyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03)	North Korea	Information theft and espionage, Sabotage and destruction, Financial crime
	Hafnium(UNC2639, UNC2640, UNC2643, Ant)	China	Information theft and espionage, Financial gain
	OilRig (Helminth, Clayslide, APT34, IRN2, COBALT GYPSY, ITG13, CHRYSENE, HEXANE, LYCEUM, HELIX KITTEN)	Iran	Information theft and espionage, Financial gain

Targeted Locations



Color	Targeted By
	Daixin Team; Lazarus Group; Hafnium
	Lazarus Group
	OilRig
	SideWinder
	Hafnium

Targeted Industries

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation
T1598:Phishing for Information	T1584:Compromise Infrastructure	T1190:Exploit Public-Facing Application	T1204:User Execution	T1078:Valid Accounts	T1078:Valid Accounts
T1598.002:Spearphishing Attachment	T1608:Stage Capabilities	T1078:Valid Accounts	T1059:Command and Scripting Interpreter	T1098:Account Manipulation	T1055:Process Injection
	T1608.004:Drive-by Target	T1566:Phishing	T1203:Exploitation for Client Execution	T1547:Boot or Logon Autostart Execution	T1055.001:Dynamic-link Library Injection
		T1189:Drive-by Compromise	T1569:System Services	T1547.006:Kernel Modules and Extensions	T1547:Boot or Logon Autostart Execution
					T1547.006:Kernel Modules and Extensions
					T1068:Exploitation for Privilege Escalation
					T1548:Abuse Elevation Control Mechanism
					T1548.002:Bypass User Account Control

TA0005: Defense Evasion	TA0006: Credential Access	TA0008: Lateral Movement	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1078:Valid Accounts	T1003:OS Credential Dumping	T1563:Remote Service Session Hijacking	T1071:Application Layer Protocol	T1567:Exfiltration Over Web Service	T1486:Data Encrypted for Impact
T1550:Use Alternate Authentication Material		T1563.001:SSH Hijacking	T1071.001:Web Protocols	T1041:Exfiltration Over C2 Channel	T1489:Service Stop
T1550.002:Pass the Hash		T1563.002: RDP Hijacking	T1584.006:Web Services		T1471 :Data Encrypted for Impact
T1140: Deobfuscate/ Decode Files or Information		T1550:Use Alternate Authentication Material	T1572:Protocol Tunneling		
T1564:Hide Artifacts		T1550.002:Pass the Hash			
T1055:Process Injection		T1021:Remote Services			
T1055.001:Dynamic-link Library Injection		T1021.001:Remote Desktop Protocol			
T1014:Rootkit		T1021.004:SSH			
T1548:Abuse Elevation Control Mechanism		T1210:Exploitation of Remote Services			
T1548.002:Bypass User Account Control					

Threat Advisories

https://www.hivepro.com/us-healthcare-organizations-targeted-by-daixin-team-ransomware/

https://www.hivepro.com/sidewinder-apt-groups-new-arsenal-named-warhawk/

https://www.hivepro.com/lazarus-neutralizes-antivirus-software-using-byovd-technique/

https://www.hivepro.com/stranger-strings-a-22-year-old-vulnerability-in-sqlite/

https://www.hivepro.com/vmware-cloud-foundation-has-a-significant-rce-flaw/

https://www.hivepro.com/threat-actors-launch-a-campaign-to-exploit-vulnerability-in-fortinet/

https://www.hivepro.com/what-can-you-do-about-the-critical-vulnerability-in-openssl-3-0/

https://www.hivepro.com/lv-ransomware-exploited-proxyshell-to-target-jordan/

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.

REPORT GENERATED ON

October 31, 2022 • 12:31 AM

More at www.hivepro.com