Hive Pro
THREAT DIGEST

Fix What Matters to Your Business

Summary of Vulnerabilities & Threats

15-21 August 2022

The third week of August 2022 witnessed the discovery of 463 vulnerabilities out of which 17 gained the attention of Threat Actors and security researchers worldwide. Among these 17, there were 3 zero-day, and 12 vulnerabilities that are awaiting analysis on the National Vulnerability Database (NVD). The Hive Pro Threat Research Team has curated a list of 17 CVEs that require immediate action.

Further, we also observed 2 Threat Actor groups being highly active in the last week. APT-C-35, an Indian threat actor group popular for Information theft and espionage and UNC3890, an Iranian threat actor group popular for Information theft and espionage were observed targeting Israel's shipping industry. 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
463	17	2	18	12	53

Detailed Report

Interesting Vulnerabilities

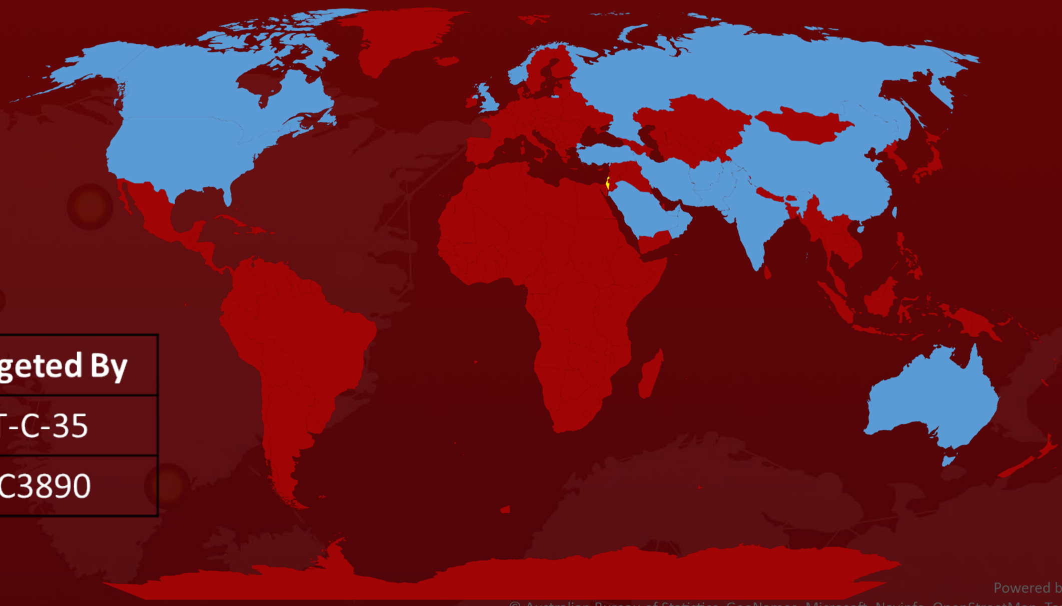
VENDOR	CVE	PATCH DETAILS
zimbra	CVE-2022-27924 CVE-2022-27925 CVE-2022-37042 CVE-2022-30333 CVE-2022-24682	https://wiki.zimbra.com/wiki/Security_Center https://www.rarlab.com/rar/rarlinux-x32-612.tar.gz
	CVE-2022-2856* CVE-2022-2852 CVE-2022-2854 CVE-2022-2855 CVE-2022-2857 CVE-2022-2858 CVE-2022-2853 CVE-2022-2859 CVE-2022-2860 CVE-2022-2861	https://www.google.com/intl/en/chrome/?standalone=1 Update to Google Chrome version 104.0.5112.101 for Mac and Linux and 104.0.5112.102/101 for Windows
	CVE-2022-32894* CVE-2022-32893*	Upgrade to macOS version 12.5.1

* zero-day vulnerability

Active Actors

ICON	NAME	ORIGIN	MOTIVE
	APT-C-35(Operation Hangover, Appin, Donot, VICEROY TIGER and SectorE02)	India	Information theft and espionage
	UNC3890	Iran	Information theft and espionage

Targeted Locations



Color	Targeted By
🔵	APT-C-35
🟡	UNC3890

Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Targeted Industries

- Financial
- Government
- Media
- NGOs
- Technology
- Defence
- Embassies
- Telecommunications
- Healthcare
- Aviation
- Transportation
- Energy

Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation
T1589: Gather Victim Identity Information	T1608: Stage Capabilities	T1195: Supply Chain Compromise	T1059: Command and Scripting Interpreter	T1053: Scheduled Task/Job	T1055: Process Injection
	T1608.004: Drive-by Target	T1566: Phishing	T1059.001: PowerShell	T1574: Hijack Execution Flow	T1053: Scheduled Task/Job
	T1106: Native API	T1566.002: Spearphishing Link	T1059.003: Windows Command Shell	T1078: Valid Accounts	T1574: Hijack Execution Flow
	T1588: Obtain Capabilities	T1091: Replication Through Removable Media	T1053: Scheduled Task/Job	T1543: Create or Modify System Process	T1068: Exploitation for Privilege Escalation
	T1588.002: Tool	T1189: Drive-by Compromise	T1053.005: Scheduled Task	T1543.003: Windows Service	T1078: Valid Accounts
	T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1203: Exploitation for Client Execution		T1543: Create or Modify System Process
	T1587.001: Malware	T1199: Trusted Relationship	T1569: System Services		T1543.003: Windows Service
		T1078: Valid Accounts	T1569.002: Service Execution		
			T1204: User Execution		
			T1204.002: Malicious File		

TA0005: Defense Evasion	TA0006: Credential Access	TA0008: Lateral Movement	TA0009: Collection	TA0010: Exfiltration	TA0011: Command and Control	TA0040: Impact
T1140: Deobfuscate/Decode Files or Information	T1056: Input Capture	T1091: Replication Through Removable Media	T1113: Screen Capture	T1020: Automated Exfiltration	T1102: Web Service	T1485: Data Destruction
T1221: Template Injection	T1056.001: Keylogging	T1210: Exploitation of Remote Services	T1056: Input Capture	T1041: Exfiltration Over C2 Channel	T1102.002: Bidirectional Communication	
T1055: Process Injection	T1056.003: Web Portal Capture		T1056.001: Keylogging	T1567: Exfiltration Over Web Service	T1105: Ingress Tool Transfer	
T1574: Hijack Execution Flow	T1555: Credentials from Password Stores		T1115: Clipboard Data		T1219: Remote Access Software	
T1070: Indicator Removal on Host	T1555.003:Credentials from Web Browsers				T1071: Application Layer Protocol	
T1078: Valid Accounts					T1071.001: Web Protocols	
					T1572: Protocol Tunneling	

Threat Advisories

https://www.hivepro.com/apt-c-35-infection-chain-adds-novel-windows-framework-modules/

https://www.hivepro.com/unknown-attackers-exploit-several-vulnerabilities-in-zimbra-collaboration-suite/

https://www.hivepro.com/chromes-zero-day-flaw-allows-arbitrary-code-execution/

https://www.hivepro.com/two-zero-day-vulnerabilities-in-macos-when-chained-can-take-over-the-entire-system/

https://www.hivepro.com/iranian-linked-hacker-group-victimized-israels-shipping-industry/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization’s attack surface before it gets exploited.

ASSETS
FOCUS
ATTACKS
VULNERABILITY

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

August 22, 2022 • 1:58 AM

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com