Hive Pro

THREAT DIGEST

Vulnerabilities & Threats that Matter
30 May - 5 June 2022

Summary

The first week of June 2022 witnessed the discovery of 412 vulnerabilities out of which 24 gained the attention of Threat Actors and security researchers worldwide. Among these 24, there were 3 zero-day and 3 other vulnerabilities about which the National vulnerability Database (NVD) is awaiting analysis while 7 were not present in the NVD at all. Hive Pro Threat Research Team has curated a list of 24 CVEs that require immediate action.

Further, we also observed 1 Threat Actor groups being highly active in the last week. TA413, a well-known Chinese threat actor group popular for information theft and espionage, was observed targeting European and Tibet-based) government and non-government organizations. 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
412	24	1	45	3	13

Detailed Report

Interesting Vulnerabilities

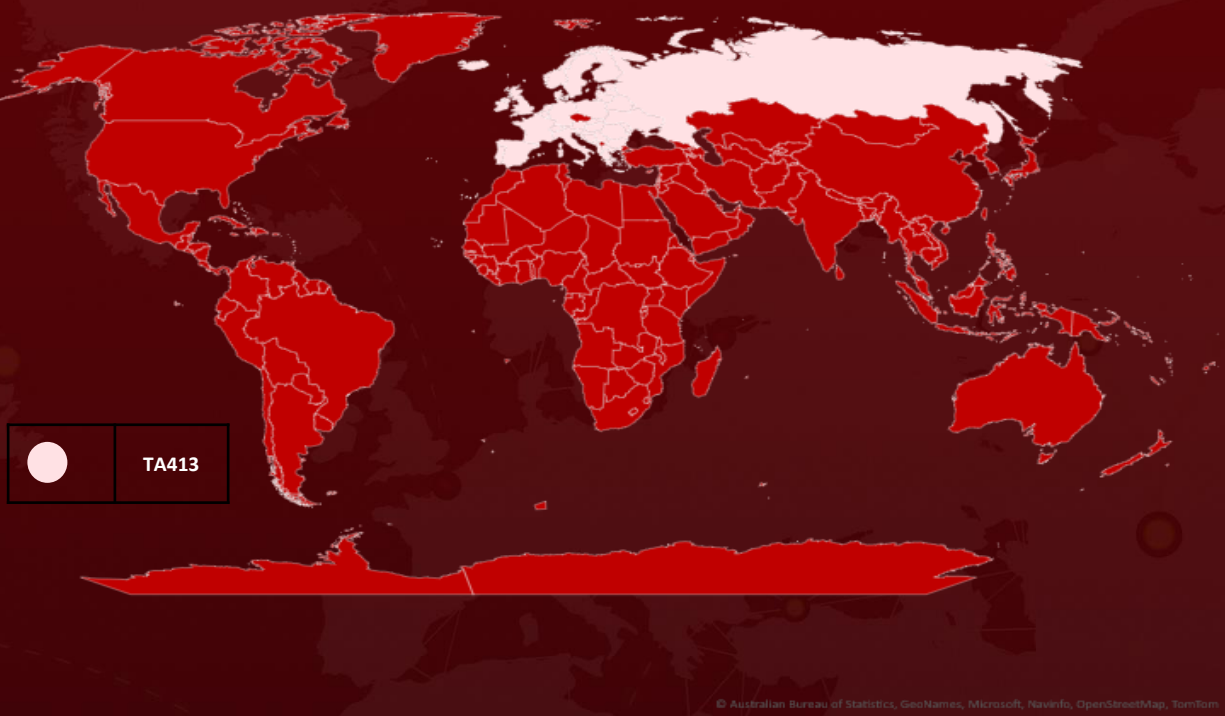
VENDOR	CVE	PATCH LINK
	CVE-2022-22784 CVE-2022-22785 CVE-2022-22786 CVE-2022-22787	https://zoom.us/download
	CVE-2022-30190*	
	CVE-2022-31736 CVE-2022-31737 CVE-2022-31738 CVE-2022-31739 CVE-2022-31740 CVE-2022-31741	https://www.mozilla.org/en-US/firefox/all/#product-desktop-release
	CVE-2021-44228* CVE-2021-45046	https://logging.apache.org/log4j/2.x/security.html
	CVE-2022-1388 CVE-2020-5902	https://support.f5.com/csp/article/K23605346 https://support.f5.com/csp/article/K52145254
	CVE-2020-7961	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/117954271
ZYXEL	CVE-2021-4039	https://www.zyxel.com/support/OS-command-injection-vulnerability-of-NWA1100-NH-access-point.shtml

VENDOR	CVE	PATCH LINK
	CVE-2022-22947	
	CVE-2022-22954	https://www.vmware.com/security/advisories/VMSA-2022-0011.html
	CVE-2021-36356	
	CVE-2022-26134*	https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html
	CVE-2022-1680 CVE-2022-1940 CVE-2022-1948	https://about.gitlab.com/update/

Active Actors

ICON	NAME	ORIGIN	MOTIVE
	TA413	China	Information theft and espionage

Targeted Locations



Targeted Industries


Government


Diplomat


NGOs

Common MITRE ATT&CK TTPs

TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0005: Defense Evasion	TA0008: Lateral Movement	TA0011: Command and Control	TA0010: Exfiltration
T1588: Obtain Capabilities	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1564: Hide Artifacts	T1210: Exploitation of Remote Services	T1132: Data Encoding	T1030: Data Transfer Size Limits
T1588.005: Exploits	T1566: Phishing	T1204: User Execution	T1564.003: Hidden Window	T1021: Remote Services	T1001: Data Obfuscation	
T1588.006: Vulnerabilities	T1566.001: Spearphishing Attachment	T1204.002: Malicious File			T1105: Ingress Tool Transfer	

Threat Advisories

https://www.hivepro.com/new-zoom-vulnerabilities-can-compromise-user-devices-with-a-single-message/

https://www.hivepro.com/follina-new-unpatched-zero-day-vulnerability-in-microsoft-office/

https://www.hivepro.com/mozilla-addresses-security-vulnerabilities-in-firefox-firefox-esr-and-thunderbird/

https://www.hivepro.com/enemybot-malware-expands-its-arsenal-by-exploiting-well-known-vulnerabilities/

https://www.hivepro.com/gitlab-addresses-critical-security-vulnerabilities-with-newer-versions/

What Next?

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

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

9 June 2022 . 5:00 AM

More at www.hivepro.com