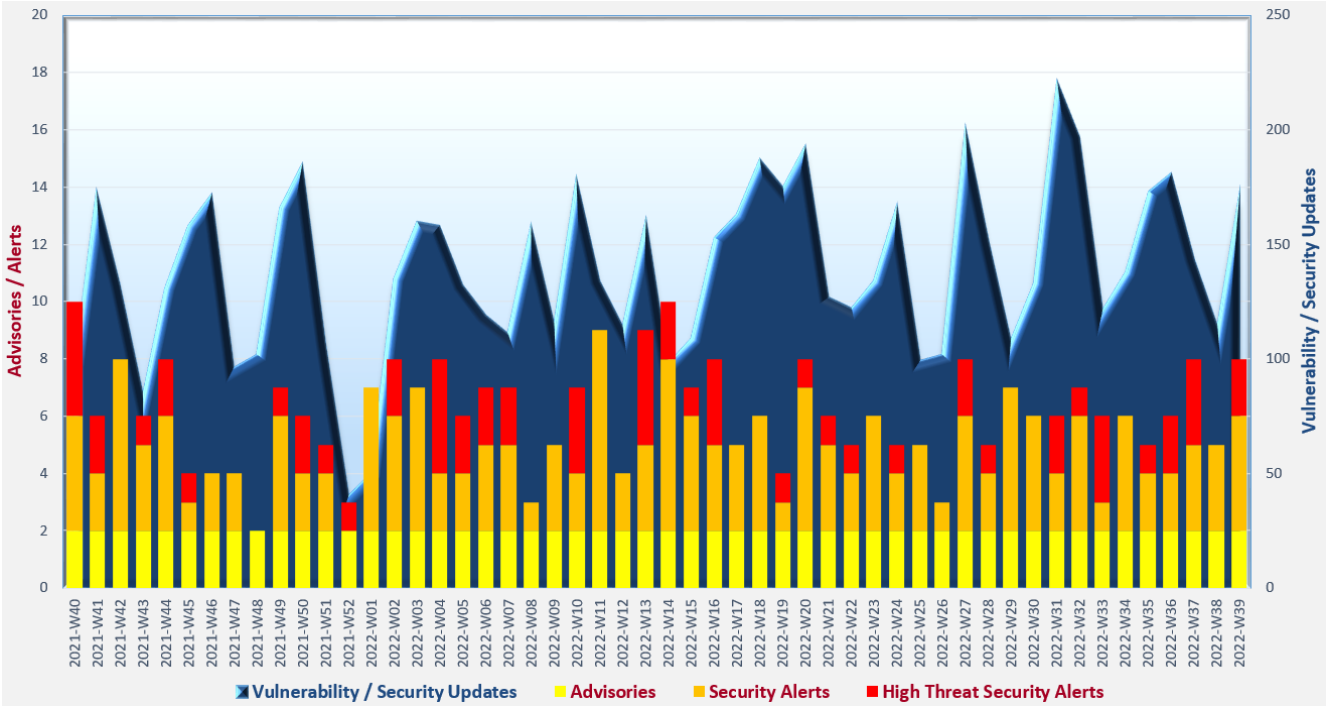
TLP:WHITE

Cyber Security Threat Trends 2022-M09

September 2022

With reference to the FIRST Traffic Light Protocol (TLP) standard[1], this document is classified as TLP:WHITE information. Recipients may share with peers and partner organisations without restriction.

Cyber Security Threat Landscape of the past 12 months (source: GovCERT.HK)



Trending:

Systems with unpatched vulnerabilities, misconfigured services or exposed Remote Desktop Protocol (RDP) are continuously targeted by attackers. System administrators should securely configure their systems, patch their systems timely, and disable internet-facing RDP, unnecessary services as well as network ports to reduce attack surfaces.

[1] https://www.first.org/tlp/

CERT Advisories

Active exploitation of vulnerabilities in various products

CERT bodies issued alerts regarding active exploitation against vulnerabilities in various products. Proof of Concept (PoC) codes for exploitation of some vulnerabilities were publicly available. System administrators should refer to vendors' documentation, apply system patches and perform mitigation measures immediately.

- GovCERT.HK[2,3], HKCERT[4,5], Cybersecurity and Infrastructure Security Agency (CISA)[6,7], Canadian Centre for Cyber Security[8,9], SingCERT[10,11], MyCERT[12,13] and JPCERT[14] issued alerts regarding multiple vulnerabilities in Microsoft Products. An elevation of privilege vulnerability (CVE-2022-37969) in Microsoft Windows and Server was being actively exploited and the technical details of an information disclosure vulnerability (CVE-2022-23960) in Microsoft Windows 11 was publicly disclosed. Two zero-day vulnerabilities (CVE-2022-41040 and CVE-2022-41082) in Microsoft Exchange Server were being actively exploited. System patch for CVE-2022-41040 and CVE-2022-41082 were not yet available as at end of September 2022. System administrators should apply the workaround recommended by Microsoft for risk mitigation.

- GovCERT.HK[15,16], HKCERT[17,18], Canadian Centre for Cyber Security[19,20] and SingCERT[21] issued alerts regarding an actively exploited vulnerability (CVE-2022-3075) in Google Chrome and Microsoft Edge (Chromium-based).

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=870
3 https://www.govcert.gov.hk/en/alerts_detail.php?id=883
4 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-september-2022
5 https://www.hkcert.org/security-bulletin/microsoft-exchange-zero-day-remote-code-execution-vulnerability_20220930
6 https://www.cisa.gov/uscert/ncas/current-activity/2022/09/13/microsoft-releases-september-2022-security-updates
7 https://www.cisa.gov/uscert/ncas/current-activity/2022/09/30/microsoft-releases-guidance-zero-day-vulnerabilities-microsoft
8 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-security-advisory-september-2022-monthly-rollup-av22-513
9 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-exchange-zero-day-vulnerabilities
10 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-050
11 https://www.csa.gov.sg/en/singcert/Alerts/al-2022-056
12 https://www.mycert.org.my/portal/advisory?id=MA-861.092022
13 https://www.mycert.org.my/portal/advisory?id=MA-866.092022
14 https://www.jpcert.or.jp/english/at/2022/at220024.html
15 https://www.govcert.gov.hk/en/alerts_detail.php?id=865
16 https://www.govcert.gov.hk/en/alerts_detail.php?id=866
17 https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20220905
18 https://www.hkcert.org/security-bulletin/microsoft-edge-security-restriction-bypass-vulnerability_20220907
19 https://www.cyber.gc.ca/en/alerts-advisories/google-chrome-security-advisory-av22-518
20 https://www.cyber.gc.ca/en/alerts-advisories/microsoft-edge-security-advisory-av22-520
21 https://www.csa.gov.sg/singcert/Alerts/al-2022-045

CERT Advisories

- GovCERT.HK[22], HKCERT[23], CISA[24], Canadian Centre for Cyber Security[25], SingCERT[26] and MyCERT [27] issued alerts regarding multiple vulnerabilities in Apple iOS and iPadOS. Vulnerability (CVE-2022-32917) was being actively exploited.

- GovCERT.HK[28], HKCERT[29] and JPCERT[30] issued alerts regarding multiple vulnerabilities in Trend Micro Apex One. Vulnerability (CVE-2022-40139) was being exploited in the wild.

- GovCERT.HK[31], HKCERT[32] and SingCERT[33] issued alerts regarding a remote code execution vulnerability (CVE-2022-3236) in Sophos Firewall. The vulnerability was being exploited in the wild.

Additional authentication method for better security

National Cyber Security Centre[34] published a guidance helping organisations on choosing a suitable type of authentication method. The guidance summarised the characteristics and application scenario of different authentication models such as multi-factor authentication, OAuth 2.0, FIDO2, magic links and one time passwords.

Blocking phishing attack

HKCERT[35] published an article on preventing phishing attack by utilising web browsers' anti-phishing website function and engine (such as Google Safe Browsing and Microsoft Defender SmartScreen). Test results of anti-phishing website function of common browsers and security advices on protection against phishing attack were provided in the article for reference.

[22] https://www.govcert.gov.hk/en/alerts_detail.php?id=869
[23] https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20220913
[24] https://www.cisa.gov/uscert/ncas/current-activity/2022/09/13/apple-releases-security-updates-multiple-products
[25] https://www.cyber.gc.ca/en/alerts-advisories/apple-security-advisory-av22-507
[26] https://www.csa.gov.sg/singcert/Alerts/AL-2022-049
[27] https://www.mycert.org.my/portal/advisory?id=MA-860.092022
[28] https://www.govcert.gov.hk/en/alerts_detail.php?id=871
[29] https://www.hkcert.org/security-bulletin/trend-micro-apex-one-multiple-vulnerabilities_20220914
[30] https://www.jpcert.or.jp/english/at/2022/at220023.html
[31] https://www.govcert.gov.hk/en/alerts_detail.php?id=878
[32] https://www.hkcert.org/security-bulletin/sophos-firewall-remote-code-execution-vulnerability_20220926
[33] https://www.csa.gov.sg/en/singcert/Alerts/al-2022-054
[34] https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type
[35] https://www.hkcert.org/blog/browser-s-anti-phishing-feature-what-is-it-and-how-it-helps-to-block-phishing-attack

Industry Insight on Cyber Security Threat Trends

Interactive intrusion activities were on the rise

Crowdstrike issued the "2022 Falcon OverWatch Threat Hunting Report"[36], which summarised their analysis and observations on threat landscape based on data collected from 1 July 2021 to 30 June 2022. The highlights from the report included:

- **A near 50% year-over-year increase in interactive intrusion campaigns was detected.** Figure for Q2 2022 was a record high as compared with previous quarterly figures. Financially motivated eCrime activity was the top threat type from July 2021 to June 2022, accounted for 43% of detected interactive intrusions. 30% of these eCrime intrusions could move laterally to more hosts within 30 minutes. 71% of all interactive intrusion activity were malware-free.

- **Technology, telecommunications and manufacturing were the top three industries most frequently targeted by interactive intrusion activity.** There were notable increases in activities targeting the healthcare and academic industries. Majority of intrusions against the healthcare industry were financially motivated eCrime activities.

- **Exploitation of public-facing infrastructure, abusing remote services such as RDP, dumping OS credentials and access to insecure credentials remained popular techniques adopted by adversaries.** Compared to the previous year, abuse of server software components, such as web shells, IIS components, etc. became more prevalent. Attackers heavily abused valid credentials for accessing and maintaining persistence in victim environments.

- **The increasing trend in number of zero-day vulnerabilities and newly disclosed CVEs continued.** More than 20,000 new vulnerabilities were reported in 2021. From January 2022 to early June 2022, the number of new vulnerabilities reported already exceeded 10,000.

- **Phishing attacks using ISO files for malware delivery became active again since late 2021.** Attackers switched their techniques in response to Microsoft's arrangement of disabling internet-enabled macros in MS Office documents by default.

Source: Crowdstrike

[36] https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/

Industry Insight on Cyber Security Threat Trends

Misconfiguration was the most popular risks observed in 2022

Censys released the "2022 State of the Internet Report"[37], which provided a comprehensive view of cyber security risks and exposures of organisations between June 2021 and June 2022 as well as guidance on strengthening security measures. The key highlights were:

- **Around 60% of observed risks were misconfigurations such as unencrypted services, weak or missing security controls and self-signed certificates.** Exposures of services, devices, and information, such as unintentional exposure of database, storage, IoT devices, credentials or API keys, accounted for 28% of observed risks. Software vulnerabilities, including end-of-life or outdated software, as well as CVEs contributed 12% of identified risks. As at June 2022, Computer and IT industry had the highest variety of risks, with over 200 distinct risk categories identified.

- **All of the top three identified risks belonged to misconfigurations.** The most common risk was services without common security headers, such as Content Security Policy (CSP), Cross-Origin Resource Sharing (CORS) or Strict Transport Security (STS), making the services vulnerable to Cross-Site Scripting (XSS) or data injection attacks. Usage of self-signed certificate not issued by trustworthy Certificate Authority was the second common risk identified. Missing identity verification could make the affected services vulnerable to man-in-the-middle attacks and phishing campaigns. Unencrypted weak authentication pages, which could be compromised by threat actors by using interception and hash cracking techniques, ranked the third in the most common risks.

- **Insecure-ssl-tls-key-length was the top risk identified in the 37 sampled medium to large organisations.** The risk was found in over 20,000 vulnerable assets.

- **As of March 2022, 5% of observed SSH services (i.e. over 10 million) still used ciphers with known vulnerabilities such as 3DES.** Organisations should use more secure ciphers such as AES for their SSH implementations.

Source: Censys

[37] https://censys.io/state-of-the-internet-report/

Industry Insight on Cyber Security Threat Trends

80% of surveyed organisations encountered serious cloud security incidents

Snyk released "The State of Cloud Security Report 2022"[38], which concluded the result of a recent survey on cloud security with more than 400 cloud engineering and security professional respondents. The key findings were:

- **4 in 5 surveyed organisations indicated that they encountered serious cloud security incidents during last year.** The incidents included data breaches, data leaks and network intrusions, which could lead to penalty for not meeting compliance standards, abuse of computing resources for crypto-mining and decrease in revenue owing to system failure. Startups (89%) and public sector (88%) were most impacted by cloud security incidents. System outage caused by improper configuration (34%) and data breach (33%) were the two most common cloud security incidents encountered. Near 90% of organisations which migrated their applications from data center to cloud platform encountered serious cloud security incidents.

- **25% of survey respondents worried that they could not notice when they encountered cloud security incidents.** 66% of security professionals and 55% of cloud engineering professionals opined that the cloud security risk would rise in the coming year. By organisation type, 69% of public sector and 66% of startups expected that cloud security risk would be higher in the coming year.

- **45% of respondents expressed that cloud security tasks consumed large amount of cloud engineer resources if there was no efficient cloud security processes in place.** Other adverse impacts included increased consumption of security personnel resources (42%) and delay in application deployment (40%). 77% of surveyed organisations expressed the major challenges in cloud security they faced were problems related to inadequate training and inefficient inter-team collaboration.

- To improve cloud security, organisations should maintain a good visibility on their cloud environments, prevent misconfiguration of their cloud resources, and adopt security by design approach and least privilege principle.

Source: Snyk

[38] https://go.snyk.io/state-of-cloud-security-2022.html

Highlight of Microsoft September 2022 Security Updates

Product Family	Impact[39]	Severity	Associated KB and / or Support Webpages
Windows 10, 11	Remote Code Execution	Critical ★★★★	KB5016616, KB5016622, KB5016623, KB5016629, KB5016639, KB5017305, KB5017308, KB5017315, KB5017327, KB5017328
Windows Server 2016, 2019, 2022 and Server Core installations	Remote Code Execution	Critical ★★★★	KB5016616, KB5016622, KB5016623, KB5016627, KB5017305, KB5017315, KB5017316, KB5017392
Windows 8.1 and Windows Server 2012, 2012 R2	Remote Code Execution	Critical ★★★★	KB5017365, KB5017367, KB5017370, KB5017377
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB5002016, KB5002017, KB5002166, KB5002178

Note: Only widely-used Microsoft products are listed and it does not mean to be inclusive. For details, please refer to https://msrc.microsoft.com/update-guide/en-us/releaseNote/2022-Sep.

Learn more:

High Threat Security Alert (A22-09-08): Multiple Vulnerabilities in Microsoft Products (September 2022) (https://www.govcert.gov.hk/en/alerts_detail.php?id=870)

[39] The Impact and Severity are the maximum impact and severity assessment of the vulnerabilities in the associated knowledgebase (KB) by Microsoft.