TLP: GREEN

CVE Trend Report

April 2023 Vulnerability Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

May 4, 2023

AhnLab

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded,
meaning that the sum of each item may not match the total.

Contents

Objectives and Scope 5

Major Statistics 5

1) CVE-2023-28206 (Apple macOS, iOS, iPadOS) 6
2) CVE-2023-2033 (Google Chrome) 7
3) CVE-2023-28252 (Windows Common Log File System) 7
4) CVE-2023-21554 (Microsoft Message Queuing) 8
5) CVE-2023-29218 (Twitter Recommendation Algorithm) 9
6) CVE-2023-27350 (PaperCut MF/NG) 9
7) CVE-2023-29489 (cPanel) 9
8) CVE-2021-44228 (Apache Log4j) 10
9) CVE-2023-23397 (Microsoft Outlook) 11
10) CVE-2023-28205 (Apple macOS, iOS, iPadOS) 11

Recommendations 12

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Objectives and Scope

Following the recent abuse of vulnerabilities in various malware distributions and attacks, it is becoming more crucial to detect said information early on.

Zero-day and other various vulnerabilities are typically spread faster through social networks. AhnLab provides the trend of current vulnerabilities through the ATIP service based on the information collected by the in-house infrastructure.

Additionally, ATIP offers information on said vulnerabilities' characteristics and countermeasures through related News Clippings, ASEC Notes, analysis reports, security advisories, and more.

This report introduces the vulnerabilities that are trending each month along with their statistics and characteristics.

Major Statistics

Table 1 shows the top 10 CVE vulnerabilities that were ranked based on the number of times they were mentioned in April 2023.

	Vulnerability Categorization	Product	CVSS	Details
1	CVE-2023-28206	Apple macOS, iOS, iPadOS	8.6	Remote Code Execution
2	CVE-2023-2033	Google Chrome	8.8	Elevation of Privilege
3	CVE-2023-28252	Windows CLFS	7.8	Elevation of Privilege
4	CVE-2023-21554	Microsoft Message Queuing	9.8	Remote Code Execution
5	CVE-2023-29218	Twitter Algorithm	7.5	Denial of Service

6	CVE-2023-27350	PaperCut MF/NG	9.8	Remote Code Execution
7	CVE-2023-29489	cPanel	5.3	Remote Code Execution
8	CVE-2021-44228	Apache Log4j	10	Remote Code Execution
9	CVE-2023-23397	Microsoft Outlook	9.8	Remote Code Execution
10	CVE-2023-28205	Apple macOS, iOS, iPadOS	8.8	Remote Code Execution

Table 1. April 2023 CVE statistics

Figure 1 is a graph that shows the trends of major vulnerabilities in April. From this, we can see the period when certain vulnerabilities became major issues as well as their trend distributions.

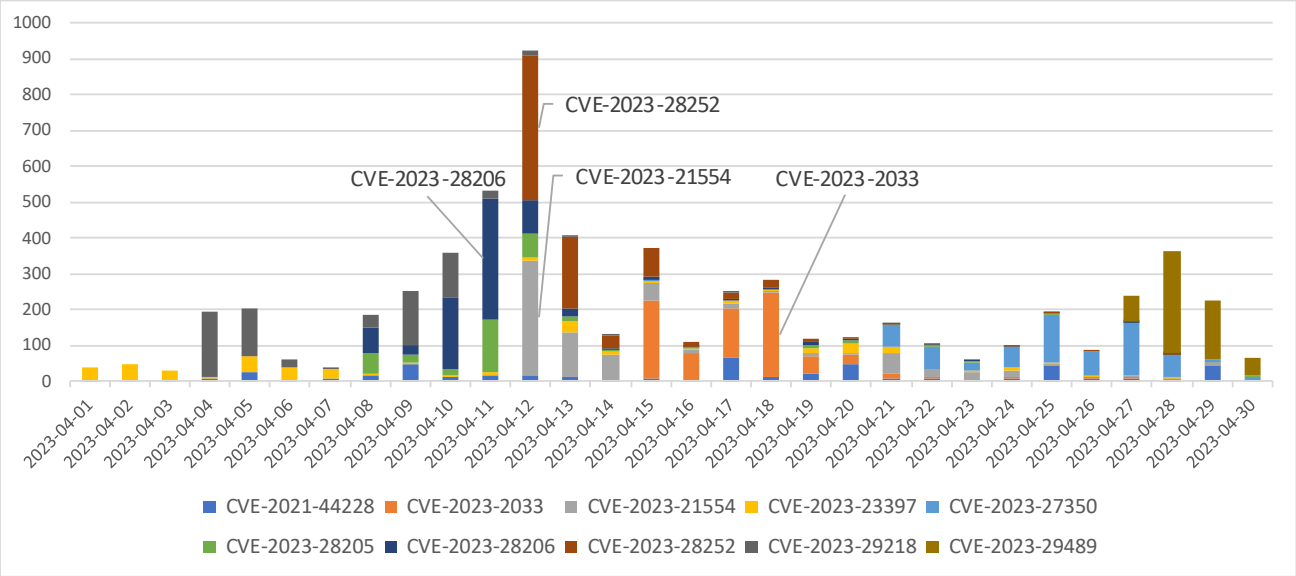

Figure 1. April 2023 CVE trends

1) CVE-2023-28206 (Apple macOS, iOS, iPadOS)

CVE-2023-28206 is an arbitrary code execution vulnerability that occurs in Apple iOS, macOS, and iPadOS; it is classified as a high-risk group with a CVSS score of 8.6. This zero-day vulnerability was exploited in an actual attack before the security patch on April 7. Its PoC code

was released on April 8 after the security patch was provided, and according to the announcement from Google Threat Analysis Group (TAG), arbitrary code execution is possible through the app installed on the operating system.

Furthermore, the April security patch included another zero-day vulnerability (CVE-2023-28205) that occurs in the WebKit module.

- April 2023 First Security Update Advisory for Apple Products[1]

2) CVE-2023-2033 (Google Chrome)

CVE-2023-2033 is the first zero-day vulnerability to occur in the Google Chrome browser in 2023, and an emergency security patch was provided on April 14. Google TAG classified it as a Type Confusion vulnerability occurring in Chrome's V8 module and stated that it influenced Windows, Linux, and macOS.

The vulnerability may be found in browsers that use the open-source Chromium engine, including Chrome, Microsoft Edge, Opera, and Naver Whale. Therefore, users must always update their browsers to the latest versions to protect themselves from potential vulnerability attacks.

- Caution Advised for Chromium-based Browser Vulnerability (CVE-2023-2033, CVE-2023-2136)[2]
- Security Update Advisory for Google Chrome (112.0.5615.121)[3]

3) CVE-2023-28252 (Windows Common Log File System)

CVE-2023-28252 is an elevation of privilege vulnerability that occurs in the Windows

[1] https://atip.ahnlab.com/ti/contents/security-advisory?i=232160bb-2182-4c68-a410-7befbe9e135c
(This report supports Korean only for now)

[2] https://atip.ahnlab.com/ti/contents/asec-notes?i=6b95ef08-44d2-46b3-b6ab-79fec0411553

[3] https://atip.ahnlab.com/ti/contents/security-advisory?i=57564c7e-5c7f-448f-b689-8574b8a3b98b
(This report supports Korean only for now)

Common Log File System (CLFS), and a security patch was provided on April 11. The CLFS is a basic feature of Windows for the logging of applications, and the vulnerability can be exploited to elevate the privilege to the SYSTEM level. The United States Cybersecurity and Infrastructure Security Agency (CISA) announced on April 11 that the vulnerability was being exploited in actual attacks[4] and advised users to conduct security checks.

- Caution Advised for Elevation of Privilege Vulnerability Using CLFS (CVE-2023-28252)[5]
- April 2023 Regular Security Update Advisory for MS Products[6]

4) CVE-2023-21554 (Microsoft Message Queuing)

CVE-2023-21554 is a remote code execution vulnerability that occurs in the Microsoft Message Queuing (MSMQ) service. It has a CVSS risk score of 9.8 and is classified as an extremely high-risk vulnerability. Threat actors can remotely perform arbitrary operations without prior authentication by sending a manipulated MSMQ packet. MSMQ does not activate in default Windows settings; however, the scope of the damage is likely to expand if the vulnerability starts to operate as it affects Windows 11 and the latest version of Windows Server 2022.

As of May 3, there are no less than 270,000 systems with active TCP port 1081 of the MSMQ service, and we confirmed that the service was activated upon the installation of the MS Exchange mail server, cloud storage used by numerous companies.

- April 2023 Regular Security Update Advisory for MS Products[7]

[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[5] https://atip.ahnlab.com/ti/contents/asec-notes?i=28704071-acd0-40b9-9245-e161d1d63e86

[6] https://atip.ahnlab.com/ti/contents/security-advisory?i=305beebd-b149-45ed-acaa-c9aaf61c4091
(This report supports Korean only for now)

[7] https://atip.ahnlab.com/ti/contents/security-advisory?i=305beebd-b149-45ed-acaa-c9aaf61c4091
(This report supports Korean only for now)

5) CVE-2023-29218 (Twitter Recommendation Algorithm)

This is a denial-of-service vulnerability that may occur due to unfollowing, blocking, or reporting certain accounts through exploitations of Twitter's recommendation algorithm feature, and a security patch was provided on April 4 through a Twitter update. Threat actors can abuse the feature to create groups of Twitter users who share similar interests and perform acts on specific accounts, such as unfollowing, muting, blocking, and reporting. Such activities are enabled by taking advantage of the recommendation algorithm's ability to deactivate accounts according to groupthink results.

- Warning for Twitter Recommendation Algorithm Vulnerability (CVE-2023-29218)[8]

6) CVE-2023-27350 (PaperCut MF/NG)

This is a remote code execution vulnerability that occurs in PaperCut MF/NG, a software for paperwork management, and a patch was provided on March 8. Later, the vulnerability was exploited by threat actors. As an n-day attack utilized for attacks after the patch, various kinds of malware, such as Truebot, buhti, MoneroOcean, and Mirai, are executed as the final payload. The researchers of Horizon3 released the PoC attack code[9] on April 24.

- Caution Advised for Vulnerabilities Exploited in Actual Attacks (Apr. 21, 2023)[10]

7) CVE-2023-29489 (cPanel)

Discovered in cPanel, a web hosting control panel software, this vulnerability is triggered by

[8] https://atip.ahnlab.com/ti/contents/security-advisory?i=d1d94045-6d20-406b-bc0c-b8bd12742d06
(This report supports Korean only for now)

[9] https://www.horizon3.ai/papercut-cve-2023-27350-deep-dive-and-indicators-of-compromise/

[10] https://atip.ahnlab.com/ti/contents/security-advisory?i=33cffc57-af2a-43dd-8a48-615292867fc8
(This report supports Korean only for now)

the XSS occurring in the cpsrvd error page from a wrong webcall ID. On April 26, Assetnote[11] released a PoC code including an analysis of its cause. Direct updates are not required for the user as the automatic update feature of cPanel is activated as a default setting; if not, the feature must be activated by referring to an article titled "How to re-enable automatic updates".[12]

- cPanel Security Update Advisory (CVE-2023-29489)[13]

8) CVE-2021-44228 (Apache Log4j)

Also known as Log4Shell, CVE-2021-44228 has been defenseless to attacks since the first report on its exposure on November 24, 2021, until an update for the Log4j 2.15.0 version was provided on December 10. During that period, no other prevention measures were provided aside from a temporary measure of deactivating the library where the vulnerability occurred, which further expanded the scope of the damage.

The vulnerability became an issue after 8220 Gang was found using the Log4Shell vulnerability to install CoinMiner.

- Analysis Report on CVE-2021-44228 Vulnerability[14]
- Q4 2021 Vulnerability Trend Report[15]
- Log4Shell (Log4j) Remote Code Execution Vulnerability (CVE-2021-44228)[16]

---

[11] https://blog.assetnote.io/2023/04/26/xss-million-websites-cpanel/

[12] https://support.cpanel.net/hc/en-us/articles/360053076314-How-to-re-enable-automatic-updates

[13] https://atip.ahnlab.com/ti/contents/security-advisory?i=c4261d5f-36bc-47e2-8a01-0173949538ae (This report supports Korean only for now)

[14] https://atip.ahnlab.com/ti/contents/issue-report/vulnerability?i=adb85e0e-2809-4e67-8e82-11a1c1d28d01

[15] https://atip.ahnlab.com/ti/contents/issue-report/vulnerability?i=8a6e7ca0-b8d5-4962-9013-20be8d837938 (This report supports Korean only for now)

[16] https://atip.ahnlab.com/ti/contents/asec-notes?i=3bf5490b-4d4c-40b4-854b-91f701145199

- Apache Log4j Security Update Advisory[17]
- 8220 Gang Uses Log4Shell Vulnerability to Install CoinMiner[18]

9) CVE-2023-23397 (Microsoft Outlook)

The zero-day vulnerability that occurred in Microsoft's email client, Outlook, has a CVSS risk score of 9.8, placing it in the high-risk group. This vulnerability leaks NTLM hashes when the path of the sound file (UNC) used to notify users of delayed notifications in Outlook Calendar's "Reminder" feature is set to the attacker's SMB server. Even after a security patch was provided on March 14, the vulnerability was mentioned in various sources constantly during April.

- Warning for Microsoft Office Outlook Privilege Escalation Vulnerability (CVE-2023-23397)[19]
- March 2023 Regular Security Update Advisory for MS Products[20]

10) CVE-2023-28205 (Apple macOS, iOS, iPadOS)

As an arbitrary code execution vulnerability occurring in the WebKit module of iOS, macOS, and iPadOS, CVE-2023-28205 has been classified as a zero-day vulnerability with CVE-2023-28206.

- April 2023 First Security Update Advisory for Apple Products[21]

---

[17] https://atip.ahnlab.com/ti/contents/security-advisory?i=0a053796-66db-4ce0-9c30-d3c19060670e
(This report supports Korean only for now)

[18] https://asec.ahnlab.com/en/51568/

[19] https://atip.ahnlab.com/ti/contents/asec-notes?i=21b1e084-6184-4409-a9ed-86088279ef72

[20] https://atip.ahnlab.com/ti/contents/security-advisory?i=dc4d37f2-b906-4330-9d32-01eeb8db3bc8
(This report supports Korean only for now)

[21] https://atip.ahnlab.com/ti/contents/security-advisory?i=232160bb-2182-4c68-a410-7befbe9e135c
(This report supports Korean only for now)

Recommendations

AhnLab supports various features such as the diagnosis of malicious files, abnormal activities, and detection of networks in order to prevent various invasive attacks. AhnLab V3 Endpoint products, MDP behavior detection engines, and EDR/MDS products can detect threats from various angles. Users must make sure to apply security patches and maintain latest versions on not only security products but also programs installed in the system. Additionally, users must prepare for potential breaches through regular security maintenances and strengthening of security settings for network firewalls.

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com
https://asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency response (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab