AhnLab Cyber Threat Intelligence Report

TLP: GREEN

CVE Trend Report

March 2023 Vulnerability Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Apr. 06, 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

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.

01 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.

02 Major Statistics

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

	Vulnerability Categorization	Product	CVSS	Details
1	CVE-2023-23397	Microsoft Outlook	9.8	Elevation of Privilege
2	CVE-2023-21716	Microsoft Word	9.8	Remote Code Execution
3	CVE-2023-21768	Windows Winsock Driver	7.8	Elevation of Privilege
4	CVE-2023-27532	Veeam Backup&Replication	7.5	Remote Code Execution

5	CVE-2023-23752	Joomla	5.3	Remote Service Access
6	CVE-2023-25610	Fortinet FortiOS, FortiProxy	9.3	Arbitrary Code Execution
7	CVE-2022-41328	Fortinet FortiOS	7.1	Arbitrary Code Execution
8	CVE-2023-23415	Windows ICMP	9.8	Remote Code Execution
9	CVE-2023-28432	MinIO	7.5	Data Leak
10	CVE-2023-0179	Linux Kernel	7.8	Arbitrary Code Execution

Table 1. March 2023 CVE statistics

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

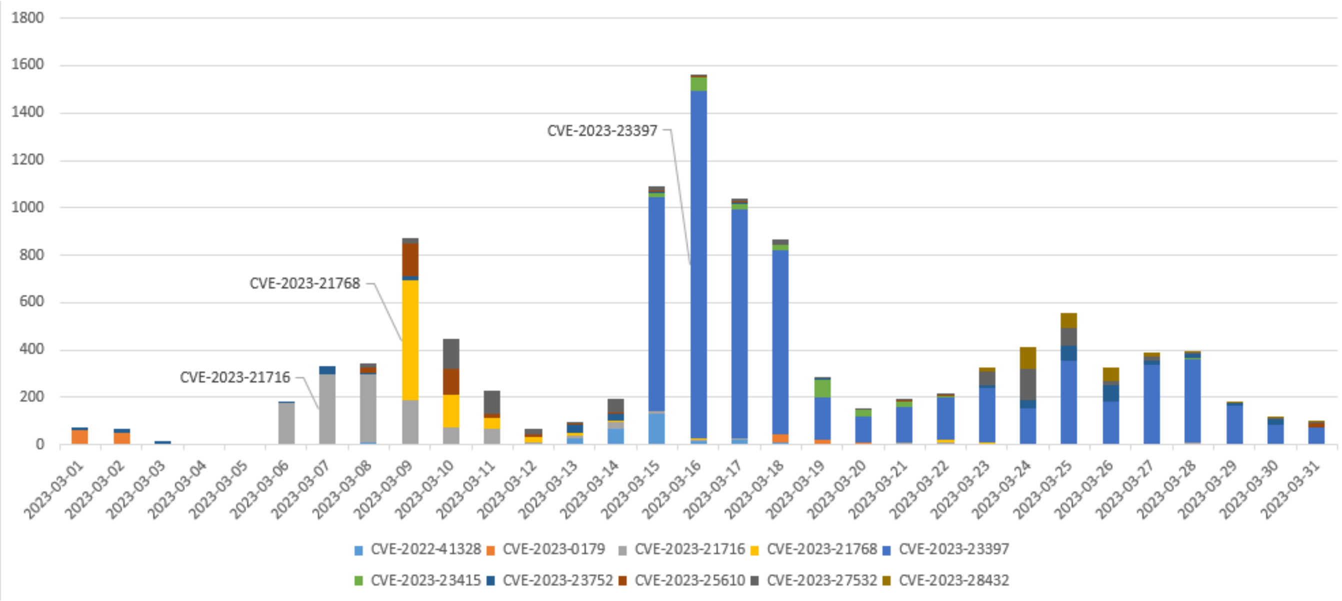

Figure 1. March 2023 CVE trends

1) CVE-2023-23397 (Microsoft Outlook)

The zero-day vulnerability that occurred in Microsoft's email client, Outlook, scored 9.8 in the CVSS risk score, 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.

The attack code for this vulnerability was discovered before the security patch that took place on March 14. It was deemed the biggest issue of March due to the fact that it was triggered even when the user did not open their email.

- Warning for Microsoft Office Outlook Privilege Escalation Vulnerability (CVE-2023-23397)
- March 2023 Regular Security Update Advisory for MS Products (This report supports Korean only for now.)

2) CVE-2023-21716 (Microsoft Word)

A security patch for the remote code execution vulnerability in Microsoft Word was provided on February 14. A security researcher from Arctic Wolf Labs revealed the POC code on March 5, and this force-quits Word if the user opens an RTF document created with malicious intentions.
Microsoft stated through their security advisory that the chances of said vulnerability being exploited are low, but there is a possibility that it could be through Outlook's preview window.

- February 2023 Regular Security Update Advisory for MS Products (This report supports Korean only for now.)

3) CVE-2023-21768 (Windows Winsock Driver)

On January 10, a security patch was provided for this elevation of privilege vulnerability that occurs in the Windows Winsock driver. This vulnerability only functions in Windows 11 and Windows Server 2022 environments, so it is estimated that the damage caused by this vulnerability will be limited. Ever since the POC code was revealed on March 7 through GitHub, more references were made to the vulnerability for about a week.

- January 2023 Regular Security Update Advisory for MS Products (This report supports Korean only for now.)

4) CVE-2023-27532 (Veeam Backup & Replication)

This vulnerability occurs in Veeam Backup & Replication (a backup and recovery solution). It allows unauthenticated users to obtain encrypted credentials stored in the configuration database. A Horizon3 researcher revealed the POC code on March 24 after the patch release on March 7.

- Veeam Product Security Update Advisory (CVE-2023-27532) (This report supports Korean only for now.)

5) CVE-2023-23752 (Joomla)

As a vulnerability caused by insufficient user access control in the Joomla Content Management System (CMS), it allows unauthenticated users to access the web service endpoint remotely and freely execute codes. After the security patch was released on February 16, the POC code was revealed through GitHub on February 23, and the vulnerability was often mentioned for the entire month of March.

- Joomla Vulnerability Security Update Advisory (CVE-2023-23752) (This report supports Korean only for now.)

6) CVE-2023-25610 (Fortinet FortiOS, FortiProxy)

This is an arbitrary code execution and denial-of-service vulnerability that occurs in Fortinet products like FortiOS and FortiProxy, and a security patch was provided on March 7. It allows unauthorized threat actors to use manipulated network requests to trigger a buffer overflow in the Fortinet product GUI. Depending on the product version of FortiOS and FortiProxy, the service is force-terminated, so additional malicious behaviors do not occur.

- March 2023 Security Update Advisory for Fortinet Products (FortiAnalyzer, FortiAuthenticator, FortiDeceptor, etc.)

7) CVE-2022-41328 (Fortinet FortiOS)

This is an arbitrary code execution vulnerability that occurs in Fortinet FortiOS, and a security patch was released on March 7. It allows access to files outside of the allowed range during the process of the input path name.

According to security company Mandiant's announcement on March 16, the China-based threat group known as UNC3886 launched an actual attack in the zero-day state. Servers with vulnerable security policies or no EDR products were the main targets, and various attacks were reported consistently.

- March 2023 Security Update Advisory for Fortinet Products (FortiAnalyzer, FortiAuthenticator, FortiDeceptor, etc.)

8) CVE-2023-23415 (Windows ICMP)

This is a remote code execution vulnerability that occurs in Windows Internet Control Message Protocol (ICMP). It has a CVSS risk score of 9.8 and is considered an extremely high-risk vulnerability. A security patch for this vulnerability was released on March 14. Threat actors can send a manipulated ICMP packet to the target server to intentionally cause errors while processing internal IP headers.

- March 2023 Regular Security Update Advisory for MS Products

9) CVE-2023-28432 (MinIO)

This is a data leak vulnerability that occurs in an open-source object storage server, MinIO, and a security patch was provided on March 20. The vulnerability exists in the administrator secret key and the route password being exposed in plain text due to the insufficient processing of the MinIO server framework's certain environment variable. The POC code was revealed on March 24 through Twitter, which made it an issue for about a week.

- MinIO Server Product Security Update Advisory (CVE-2023-28432) (This report supports Korean only for now.)

10) CVE-2023-0179 (Linux Kernel)

This is a stack buffer overflow vulnerability that occurs in the Linux kernel NetFilter package, Net/NetFilter/nft_payload.c, and a security patch was released on January 13. This vulnerability is triggered by the insufficient verification of integer type calculation when designating Virtual Local Area Network (VLAN) as a tag in the nftables feature that processes network packets. This allows access to the kernel memory due to return values exceeding that of the data type caused by incorrect calculations.
The POC code was revealed through Twitter on February 28, and there were increased references made to this vulnerability until early March.

- Linux Kernel (Netfilter) Package Security Update Advisory (CVE-2023-0179) (This report supports Korean only for now.)

AhnLab supports various features such as the diagnosis of malicious files, abnormal behaviors, 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