AhnLab Cyber Threat Intelligence Report

TLP: GREEN

CVE Trend Report

May 2023 Vulnerability Statistics and Major Issues

V1.0

AhnLab Security Emergency response Center (ASEC)

Jun. 12, 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.

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. Based on the information collected through in-house infrastructure, trends on vulnerabilities currently in the spotlight are provided through ATIP services.

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 CVEs that were ranked based on the number of times they were mentioned in May 2023.

	Vulnerability Categorization	Product	CVSS	Details
1	CVE-2023-24932	Windows Secure Boot	6.7	Security Feature Bypass
2	CVE-2023-32784	KeePass	7.5	Cleartext Storage of Sensitive Information
3	CVE-2023-27350	PaperCut NG/MF	9.8	Remote Code Execution
4	CVE-2023-2825	GitLab CE/EE	7.5	Remote Code Execution
5	CVE-2023-28929	Trend Micro Security	8.6	Remote Code Execution

6	CVE-2023-25717	Ruckus Wireless AP	9.8	Remote Code Execution
7	CVE-2023-32233	Linux Kernel Netfilter	7.8	Elevation of Privilege
8	CVE-2023-27363	Foxit Reader	7.8	Remote Code Execution
9	CVE-2023-28771	Zyxel VPN/Firewall	9.8	Remote Code Execution
10	CVE-2023-25690	Apache HTTP Server	9.8	Access Control Bypass

Table 1. May 2023 CVE statistics

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

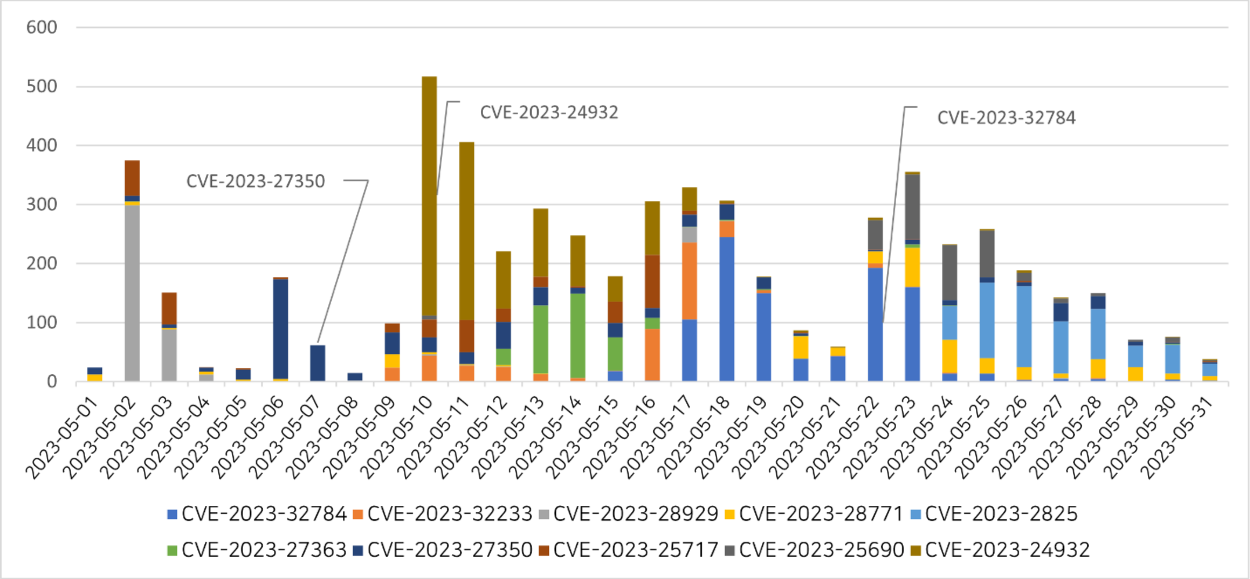

Figure 1. May 2023 CVE trends

1) CVE-2023-24932 (Windows Secure Boot)

This is a vulnerability that allows the bypassing of the Windows Secure Boot feature. It is actually in use by the BlackLotus UEFI bootkit malware. As a bootkit is executed before the operating system is loaded, it can hinder or deactivate various security mechanisms in operating systems such as BitLocker, Hypervisor-Protected Code Integrity (HVCI), and Microsoft Defender.

Windows provided the Secure Boot feature that checks the signature of the booting software to defend against UEFI manipulation by threat actors which has been occurring for quite some time.[1] However, it is important to recognize that it is not perfectly safe against UEFI modification attacks due to frequently identified vulnerabilities that allow this security feature to be bypassed.

The security update on May 9, 2023, only offers an option to manually turn on the protective mechanism against this vulnerability and does not automatically enable the feature. Also, the method of manual activation is complex and has the potential to harm the system, leading to Windows users and security researchers raising complaints about such a patch method.

- May MS Security Patch Vulnerability Information[2]
- May 2023 Regular Security Update Advisory for MS Products[3]

2) CVE-2023-32784 (KeePass)

This is a vulnerability that arises in KeePass, an open-source password manager. By exploiting this vulnerability, threat actors can obtain the master password key even if the workspace is locked or KeePass is not running. However, it is not possible to do so remotely and it requires the KeePass process, swap file (pagefile.sys), hibernation file (hiberfil.sys) or the RAM of the entire system to be dumped within the system.

This vulnerability became an issue when the POC code was published on GitHub under the name KeePass 2.X Master Password Dumper.

- KeePass Security Update Advisory (CVE-2023-32784)[4]

[1] https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot

[2] https://atip.ahnlab.com/ti/contents/asec-notes?i=3a62e681-92ea-4263-be39-ccb2aa695342

[3] https://atip.ahnlab.com/ti/contents/security-advisory?i=15d16a5d-436b-4350-b12f-8500c1e3bbe7

(This report supports Korean only for now)

[4] https://atip.ahnlab.com/ti/contents/security-advisory?i=be34706f-0c33-4eae-8ee9-20afda08f545

(This report supports Korean only for now)

3) CVE-2023-27350 (PaperCut)

This is a remote code execution vulnerability that arises in PaperCut MF/NG, print management software, and a patch was released on March 8. The vulnerability continued to be exploited by threat actors and became an issue again in May following April. By exploiting this vulnerability, threat actors execute various malware such as CLOP Ransomware, Bl00dy Ransomware, and MoneroOcean as the final payload.

The cause of this vulnerability is poor access control within the SetupCompleted java class, allowing threat actors to bypass authentication and access the server as an admin. For more related details, please refer to the AhnLab TIP analysis report.

- Analysis Report on CVE-2023-27350 Vulnerability[5]
- April 2023 CVE Trend Report[6]
- Warning Against Vulnerability Exploited in Actual Attacks (Apr. 21, 2023)[7]

4) CVE-2023-2825 (GitLab CE/EE)

This is a path traversal vulnerability that arises in GitLab CE/EE, a web-based DevOps platform. It allows an unauthorized malicious user to insert multiple instances of the string "..%2f" in the uploaded file path and read files within the server. The exploitation of this vulnerability enables threat actors to read files, credentials, and keys, so there is the potential for this to cause not only information leakage from the GitLab server but also privilege escalation and remote code execution.

[5] https://atip.ahnlab.com/ti/contents/issue-report/vulnerability?i=e753784a-e766-472f-a01d-f071cf27b6b7

(This report supports Korean only for now)

[6] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=3e23eaed-8f7f-4c32-bf93-7bd1f066964c

[7] https://atip.ahnlab.com/ti/contents/security-advisory?i=33cffc57-af2a-43dd-8a48-615292867fc8

(This report supports Korean only for now)

- GitLab CE/EE Security Update Advisory (CVE-2023-2825)[8]

5) CVE-2023-28929 (Trend Micro Security)

CVE-2023-28929 is a DLL hijacking vulnerability; when a certain file is executed, malware placed by the threat actor is launched, and persistence can also be maintained. Trend Micro stated that there have been no identified cases of its exploitation in actual attacks. This vulnerability became an issue after being identified during research by NTT Security Holdings, and it affects Trend Micro Security 2022/2023 (versions 17.7.1476 or earlier) and Trend Micro Security 2021 (versions 17.0.1412 or earlier).

6) CVE-2023-25717 (Ruckus Wireless AP)

This is a remote code execution vulnerability that arises in a wireless router from Ruckus. It is triggered when threat actors send a malicious GET request to a device where web components are activated. It has a CVSS score of 9.8.

This vulnerability was identified on Feb 8, 2023, but the devices characteristically render the process of identifying those affected by this vulnerability and applying an update that can be bothersome. Accordingly, a botnet malware called AndoryuBot that exploits this vulnerability was being actively distributed since mid-April.

- RUCKUS AP Web Vulnerability Security Update Advisory (CVE-2023-25717)[9]

[8] https://atip.ahnlab.com/ti/contents/security-advisory?i=a466debc-e01a-40c4-95de-26b8078fdc5e

(This report supports Korean only for now)

[9] https://atip.ahnlab.com/ti/contents/security-advisory?i=2b3d7101-3737-46e1-a34e-ced722859758

(This report supports Korean only for now)

7) CVE-2023-32233 (Linux Kernel Netfilter)

This is an elevation of privilege vulnerability that arises in Linux kernel. A use-after-free (UAF) vulnerability is triggered when Netfilter's nf_tables, which inspects network packet filtering and implements network address translation rules, processes a batch request. A local user with ordinary permissions could use this vulnerability to obtain root privileges. There is a variety of operating systems based on Linux kernel which is widely used, so we predict that the vulnerability will have a wide scope of impact.

The exploit code was released alongside a brief technical analysis. Users of vulnerable versions are advised to follow the security advisory below and run the update.

- Linux Kernel Security Update Advisory (CVE-2023-32233)[10]

8) CVE-2023-27363 (Foxit Reader)

Foxit Reader is a PDF viewer used as an alternative to Adobe's PDF document reader. This vulnerability arises when the Javascript interface which allows writing to arbitrary files within the exportXFAData method is exposed. Opening a PDF which is made to drop a malicious file in the Startup folder will allow arbitrary codes to be executed when the user reboots the system.

It became an issue after its POC was released on GitHub on May 12, and as of the date of this report being written, there are no known cases of its use in actual attacks.

9) CVE-2023-28771 (Zyxel VPN / Firewall)

Zyxel is a network solutions provider, and the vulnerability arises in the company's VPN and firewall. It is a remote code execution vulnerability that arises due to poor error message

[10] https://atip.ahnlab.com/ti/contents/security-advisory?i=ef4ca3b3-726c-4309-9216-45bb29b44075

(This report supports Korean only for now)

processing in the IKEv2 packet decoder component used for VPN connections. The POC was released on May 19 along with a technical analysis, and a week later, on May 26, it became known that a Mirai-based botnet which exploits this vulnerability had been actively distributed, placing this vulnerability in the spotlight.

When VPN is not in use, the UDP port 500/4500 must be deactivated or the device updated to the latest version.

- Zyxel Firewall Product Line Security Update Advisory (CVE-2023-28771)[11]

10) CVE-2023-25690 (Apache HTTP Server)

This vulnerability allows HTTP request smuggling attacks in some mod_proxy structures of Apache HTTP Server versions between 2.4.0 and 2.4.55. Exploitation of this vulnerability allows the evasion of the proxy server's access control and this can potentially lead to unauthorized access and data leakage. It was given a CVSS score of 9.8, and its POC code was released on May 22.

- Apache HTTP Server Security Update Advisory (CVE-2023-25690)[12]

Summary

In April, five of the ten most mentioned vulnerabilities were those in Microsoft and Apple products, but only two such vulnerabilities made the list in May. Vulnerabilities were also found in server-related products such as PaperCut, GitLab, and Apache HTTP Server. Particularly, attacks that abuse the vulnerability in PaperCut continued in May following those in April.

[11] https://atip.ahnlab.com/ti/contents/security-advisory?i=45860099-00ed-4ef8-85d6-045b9822ea4a

(This report supports Korean only for now)

[12] https://atip.ahnlab.com/ti/contents/security-advisory?i=21a49e8a-33e1-4dfd-9176-5e9aef8796f5

(This report supports Korean only for now)

Vulnerabilities with CVSS scores of 9.8 were found in Ruckus Wireless AP, a network device, as well as in Zyxel VPN/Firewall. These were also used in actual attacks. When remote code execution vulnerabilities are triggered in network devices, they are usually infected with botnet malware, invoking a mass network traffic flow.

Aside from these, the vulnerability that arose in Trend Micro Security only became an issue among security researchers and did not have its POC code released, and the potential for its use in actual attacks is thought to be low.

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