Vulnerability Digest

April 2021

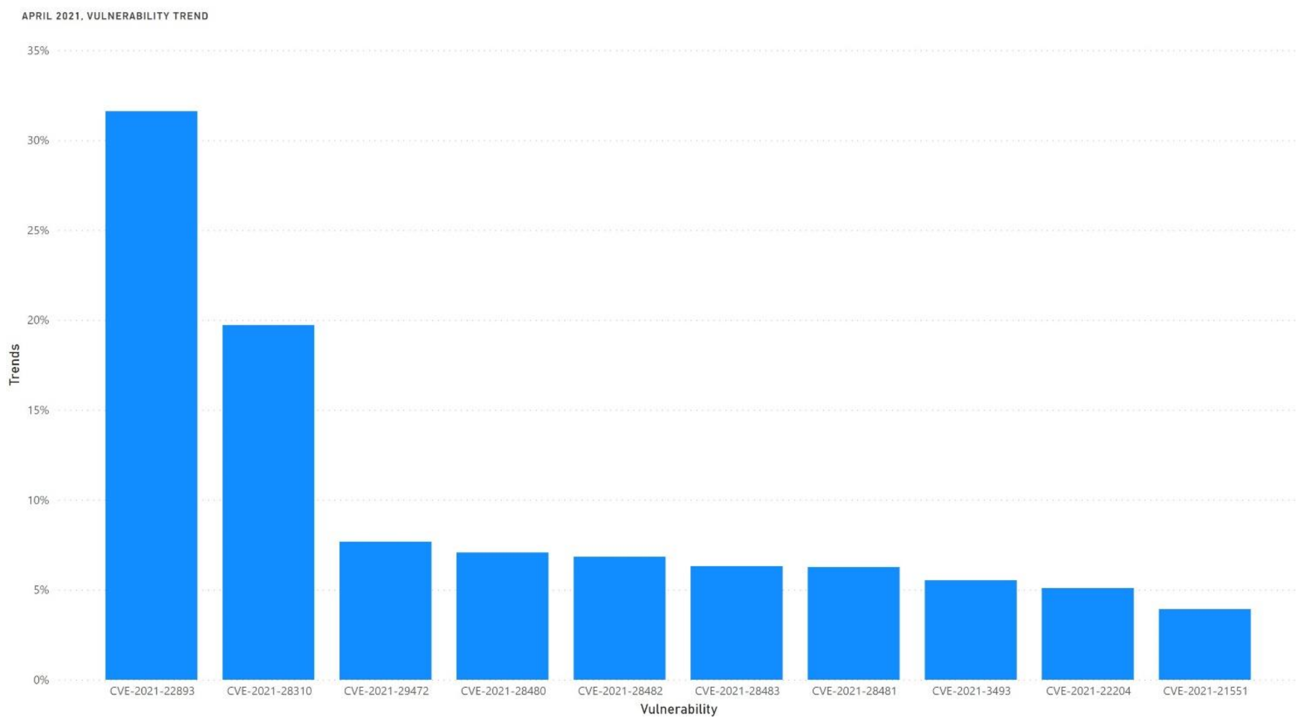
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

2563AP Den Haag, Netherlands | info@scantitan.com

SUMMARY

This report shows the monthly top 10 trends on security vulnerabilities and how hackers, malware and exploit kits are exploiting those vulnerabilities. We assign trend value as a percentage of how each vulnerability is gaining the attention of cyber security communities, attackers and malware. Companies can benefit from the report to have more cyber threat insights and anticipate attacks wave that might target their public assets in the following months.

The following chart shows the trends.



April 2021 was a relief for system admins as less critical vulnerabilities compared to previous months. Pulse Secure authentication bypass was the vulnerability of the month. The next in line is Windows Kernel privilege escalation which is currently being exploited by attackers.

Other critical and important vulnerabilities were discovered in MS Exchange Server, Composer, Dell Driver, and Linux Kernel.

The following table shows the summary of the trends.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2021-22893	Pulse Secure authentication bypass	20/04/2021	Yes	32%
CVE-2021-28310	Privilege escalation in Windows Kernel	13/04/2021	Yes	20%
CVE-2021-29472	Command injection in Composer	27/04/2021	Yes	8%
CVE-2021-28480	Remote Code Execution in Microsoft Exchange	13/04/2021	No	7%
CVE-2021-28482	Remote Code Execution in Microsoft Exchange	13/04/2021	Yes	6%
CVE-2021-28483	Remote Code Execution in Microsoft Exchange	13/04/2021	No	6%
CVE-2021-28481	Remote Code Execution in Microsoft Exchange	13/04/2021	No	6%
CVE-2021-3493	Privilege escalation in Linux Kernel	16/04/2021	Yes	6%
CVE-2021-22204	Code execution in ExifTool	23/04/2021	Yes	5%
CVE-2021-21551	Privilege escalation in Dell Driver	05/04/2021	Yes	4%

*Trends value is rounded.

Next pages show the details for each vulnerability.

CVE-2021-22893

Publish Date 20/04/2021

Exploited Yes

CVSSv3 Rate 10.0 CRITICAL

Description

Pulse Connect Secure is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure that can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway.

Links

https://blog.pulsesecure.net/pulse-connect-secure-security-update/

CVE-2021-28310

Publish Date 13/04/2021

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

Privilege escalation vulnerability in Windows kernel (Win32k) due to out-of-bounds (OOB) write issue in dwmcore.dll, which is part of Desktop Window Manager (dwm.exe).

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28310

https://securelist.com/zero-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/

https://ti.dbappsecurity.com.cn/blog/index.php/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/

CVE-2021-29472

Publish Date	23/04/2021
Exploited	Yes
CVSSv3 Rate	8.8 HIGH

Description

Command injection vulnerability exists in Composer the PHP library manager which allows supply chain attack to be successful.

Links

https://blog.packagist.com/composer-command-injection-vulnerability/

https://blog.sonarsource.com/php-supply-chain-attack-on-composer/

CVE-2021-28480

Publish Date	13/04/2021
Exploited	No
CVSSv3 Rate	9.8 CRITICAL

Description

Remote code execution vulnerability exists in Microsoft Exchange Server. By sending a special request to the server, an attacker is able to execute arbitrary code on the server. This vulnerability is unique from CVE-2021-28482, CVE-2021-28481, and CVE-2021-28483.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28480

CVE-2021-28482

Publish Date	13/04/2021
Exploited	Yes
CVSSv3 Rate	8.8 HIGH

Description

Remote code execution vulnerability exists in Microsoft Exchange Server. By sending a special request to the server, an attacker is able to execute arbitrary code on the server. This vulnerability is unique from CVE-2021-28480, CVE-2021-28481, and CVE-2021-28483.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28482

https://gist.github.com/testanull/9ebbd6830f7a501e35e67f2fcaa57bda

CVE-2021-28483

Publish Date	13/04/2021
Exploited	No
CVSSv3 Rate	9.8 CRITICAL

Description

Remote code execution vulnerability exists in Microsoft Exchange Server. By sending a special request to the server, an attacker is able to execute arbitrary code on the server. This vulnerability is unique from CVE-2021-28480, CVE-2021-28481, and CVE-2021-28482.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28483

CVE-2021-28481

Publish Date	13/04/2021
Exploited	No
CVSSv3 Rate	9.8 CRITICAL

Description

Remote code execution vulnerability exists in Microsoft Exchange Server. By sending a special request to the server, an attacker is able to execute arbitrary code on the server. This vulnerability is unique from CVE-2021-28480, CVE-2021-28482, and CVE-2021-28483.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28481

CVE-2021-3493

Publish Date	16/04/2021
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

Local privilege escalation vulnerability exists in Linux kernel as overlayfs implementation did not properly validate with respect to user namespaces the setting of file capabilities on files in an underlying file system.

Links

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=7c03e2cda4a584cadc398e8f6641ca9988a39d52

http://packetstormsecurity.com/files/162434/Kernel-Live-Patch-Security-Notice-LSN-0076-1.html

CVE-2021-22204

ExifTool

Publish Date 23/04/2021

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

Improper neutralization of user data in the DjVu file format in ExifTool allows arbitrary code execution when parsing the malicious image.

Links

https://github.com/exiftool/exiftool/commit/cf0f4e7dcd024ca99615bfd1102a841a25dde031#diff-fa0d652d10dbcd246e6b1df16c1e992931d3bb717a7e36157596b76bdadb3800

https://twitter.com/wcbowling/status/1385803927321415687

CVE-2021-21551

Publish Date 05/04/2021

Exploited Yes

CVSSv3 Rate 8.8 HIGH

Description

Dell dbutil_2_3.sys driver contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required.

Links

https://www.dell.com/support/kbdoc/en-us/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability

https://labs.sentinelone.com/cve-2021-21551-hundreds-of-millions-of-dell-computers-at-risk-due-to-multiple-bios-driver-privilege-escalation-flaws/

Subscribe to this monthly report by clicking here and prioritize your efforts on defending against cyber security attacks and threats.