Vulnerability Digest

January 2021

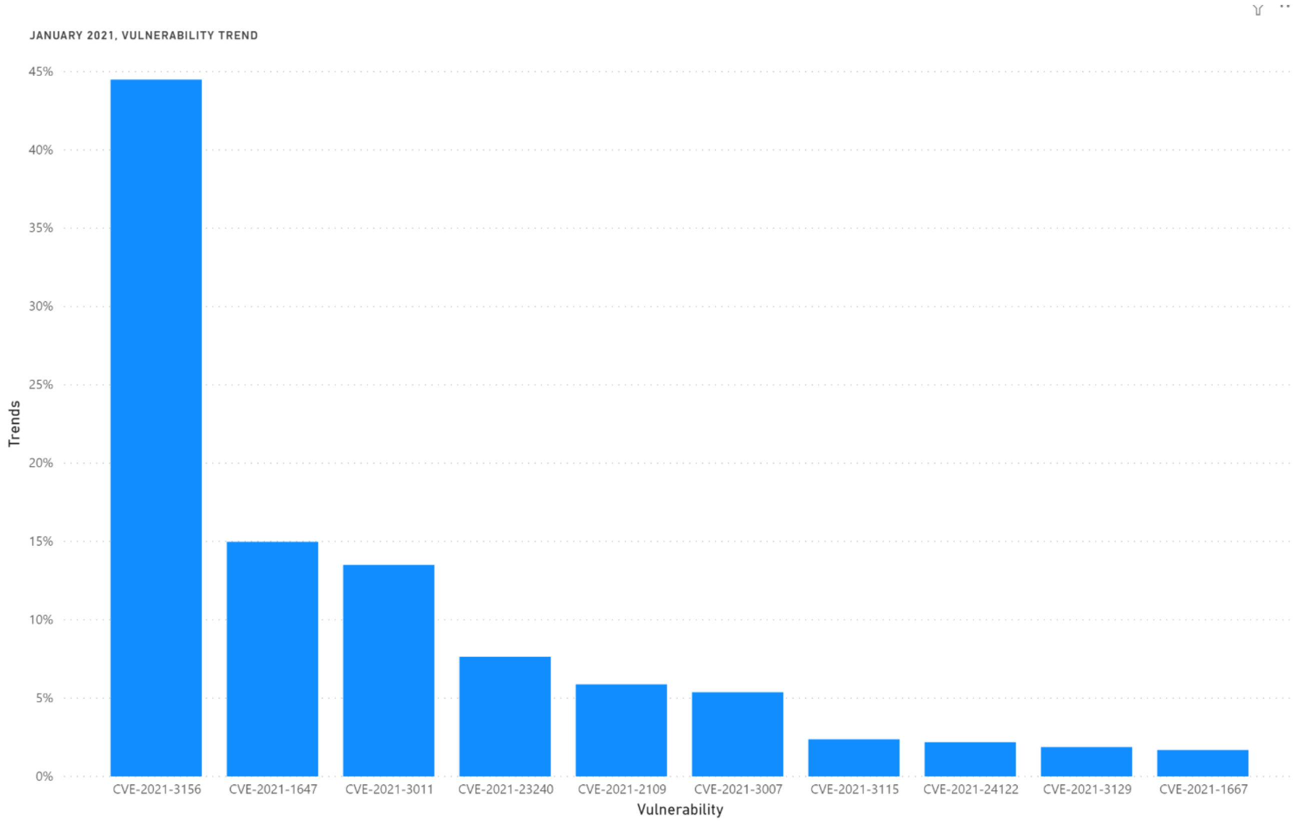
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

2524 hd 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.



Starting of 2021, we see a smaller number of vulnerabilities. However, still many remote code execution vulnerabilities in Jan 2021 were discovered and disclosed. The vulnerability with most interaction is SUDO remote code execution that is installed on most Linux environments.

The majority of Jan2021 vulnerabilities affect web technologies and frameworks like Laravel, WebLogic, TomCat, and ZendFramework.

The following table shows the summary of the trends.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2021-3156	Remote Code Execution in SUDO	26/01/2021	Yes	44%
CVE-2021-1647	Remote Code Execution in Windows Defender	12/01/2021	Yes	15%
CVE-2021-3011	Side Channel in Google Titan Security Key	07/01/2021	Yes	14%
CVE-2021-23240	Privilege Escalation in SUDO	11/01/2021	Yes	8%
CVE-2021-2109	Remote Code Execution in Oracle WebLogic	20/01/2021	Yes	6%
CVE-2021-3007	Remote Code Execution in ZendFramework	04/01/2021	Yes	5%
CVE-2021-3115	Command Execution in GoLang	19/01/2021	Yes	2%
CVE-2021-24122	JSP Source Code disclosure in Apache TomCat	14/01/2021	Yes	2%
CVE-2021-3129	Remote Code Execution in Laravel	12/01/2021	Yes	2%
CVE-2021-1667	Remote Code Execution in MS RPC	12/01/2021	No	2%

*Trends value is rounded.

Next pages show the details for each vulnerability.

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

CVE-2021-3156

Publish Date	26/01/2021
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

A heap overflow vulnerability exists in the common command sudo of Linux systems. That allow any local users to execute commands with root privilege.

Links

https://www.sudo.ws/stable.html#1.9.5p2

https://github.com/stong/CVE-2021-3156

CVE-2021-1647

Publish Date	12/01/2021
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

A remote code execution exists in Malware Protection Engine component (mpengine.dll) of Windows Defender. This is a zero-day vulnerability as it is exploited in the wild. However, no technical analysis nor PoC is available yet.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1647

CVE-2021-3011

Publish Date	07/01/2021
Exploited	Yes
CVSSv3 Rate	4.2 MEDIUM

Description

An electromagnetic-wave side-channel issue was discovered on Google Titan Security Key (2FA token) that uses NXP security microcontrollers. It allows attackers to extract the ECDSA private key after extensive physical access and consequently produce a clone.

Links

https://ninjalab.io/a-side-journey-to-titan/

CVE-2021-23240

Publish Date	11/01/2021
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

A vulnerability in sudoedit of Sudo before 1.9.5 allows a local unprivileged user to gain file ownership and escalate privileges by replacing a temporary file with a symlink to an arbitrary file target.

Links

https://www.sudo.ws/alerts/sudoedit_selinux.html

CVE-2021-2109

Publish Date	20/01/2021
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

A remote code execution vulnerability exists in console component of Oracle WebLogic Server. This vulnerability requires authentication.

Links

https://www.oracle.com/security-alerts/cpujan2021.html

https://packetstormsecurity.com/files/161053/Oracle-WebLogic-Server-14.1.1.0-Remote-Code-Execution.html

CVE-2021-3007

Publish Date	04/01/2021
Exploited	Yes
CVSSv3 Rate	9.8 CRITICAL

Description

Laminas and Zend Framework (Stream.php) has a deserialization vulnerability that can lead to remote code execution if the content is controllable by an attacker. NOTE: Zend Framework is no longer supported by the maintainer.

Links

https://github.com/laminas/laminas-http/releases/tag/2.14.2

https://github.com/Ling-Yizhou/zendframework3-/blob/main/zend%20framework3%20%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%20rce.md

CVE-2021-3115

Publish Date	19/01/2021
Exploited	Yes
CVSSv3 Rate	7.3 HIGH

Description

Go language on Windows is vulnerable to Command Injection and remote code execution when using the "go get" command to fetch modules that make use of cgo (for example, cgo can execute a gcc program from an untrusted download).

Links

https://blog.golang.org/path-security

https://github.com/golang/go/issues/43783

CVE-2021-24122

Publish Date	14/01/2021
Exploited	Yes
CVSSv3 Rate	7.5 HIGH

Description

Apache Tomcat has JSP source code disclosure in some configurations when it serves resources from network location using NTFS file system.

Links

https://tomcat.apache.org/security-10.html

CVE-2021-3129

Publish Date	12/01/2021
Exploited	Yes
CVSSv3 Rate	9.8 CRITICAL

Description

Remote code execution vulnerability exists in Ignition before 2.5.2, as used in Laravel and other products, allows unauthenticated remote attackers to execute arbitrary code because of insecure usage of file_get_contents() and file_put_contents(). This is exploitable on sites using debug mode with Laravel before 8.4.2.

Links

https://github.com/facade/ignition/pull/334

https://www.ambionics.io/blog/laravel-debug-rce

CVE-2021-1667

Publish Date	12/01/2021
Exploited	No
CVSSv3 Rate	8.8 HIGH

Description

A remote code execution vulnerability exists in Remote Procedure Call of Microsoft.

Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1667

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