Vulnerability Digest
December 2020

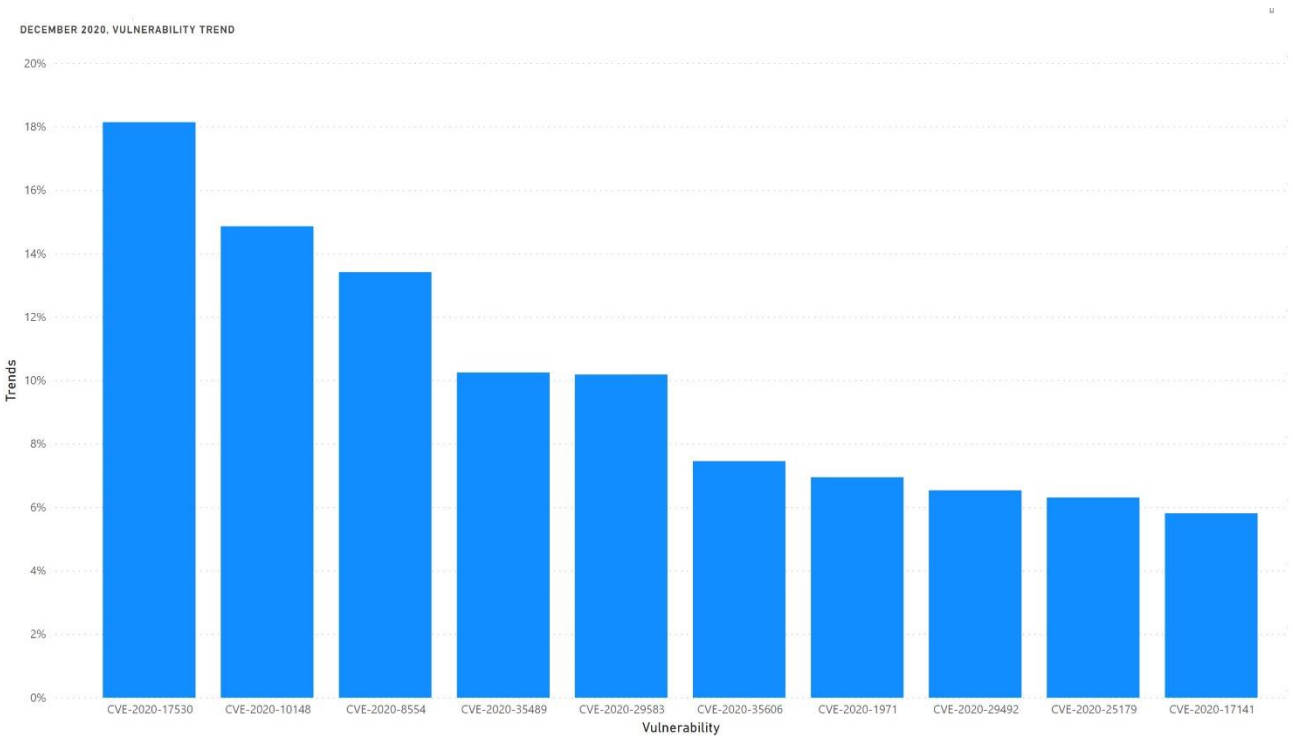
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

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.



In December 2020, SolarWinds cybersecurity news grabbed the majority of community attention due to the impact that happened on big organizations, security companies, and government entities that use SolarWinds products.

However, 2020 ended with many other critical security vulnerabilities like Struts 2 RCE and Contact Form 7 arbitrary file upload.

The following table shows the summary of the trends.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2020-17530	Remote Code Execution in Struts 2	08/11/2020	Yes	18%
CVE-2020-10148	Remote Code Execution in SolarWinds	26/11/2020	Yes	15%
CVE-2020-8554	MiTM in Kubernetes	07/11/2020	Yes	14%
CVE-2020-35489	Arbitrary File Upload in Contact Form 7	17/11/2020	Yes	10%
CVE-2020-29583	Default Account in ZYXEL devices	22/11/2020	Yes	10%
CVE-2020-35606	Command Execution in Webmin	21/11/2020	Yes	7%
CVE-2020-1971	Denial of Service in OpenSSL	08/11/2020	No	7%
CVE-2020-29492	Insecure Configuration in Wyse Dell	21/11/2020	Yes	7%
CVE-2020-25179	Unprotected Credentials in GE Ultrasound Products	09/11/2020	No	6%
CVE-2020-17141	Remote Code Execution in MS Exchange Server	09/11/2020	Yes	6%

*Trends value is rounded.

Next pages show the details for each vulnerability.

CVE-2020-17530

Publish Date 08/12/2020

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

Apache Struts 2 has remote code execution vulnerability when using forced OGNL evaluation on untrusted user input. This affects Struts 2.0.0 - Struts 2.5.25.

Links

https://cwiki.apache.org/confluence/display/WW/S2-061

https://github.com/fengziHK/CVE-2020-17530-strust2-061

CVE-2020-10148

Publish Date 26/12/2020

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

The SolarWinds Orion API is vulnerable to authentication bypass which allows remote code execution without requiring authentication. This vulnerability is known as SUNBURST backdoor.

Links

https://kb.cert.org/vuls/id/843464

https://www.solarwinds.com/securityadvisory

CVE-2020-8554

Publish Date 07/12/2020

Exploited Yes

CVSSv3 Rate 6.3 MEDIUM

Description

Man-in-The-Middle vulnerability exists in Kubernetes which affects mainly multitenant deployments where a user with no special permission is able to exploit this vulnerability.

Links

https://github.com/kubernetes/kubernetes/issues/97076

https://blog.champtar.fr/K8S_MITM_LoadBalancer_ExternalIPs/

CVE-2020-35489

Publish Date 17/12/2020

Exploited Yes

CVSSv3 Rate 10.0 CRITICAL

Description

Unrestricted file upload vulnerability exists in Contact Form 7 the common WordPress plugin where there is no validation for Unicode special character.

Links

https://contactform7.com/2020/12/17/contact-form-7-532/

https://github.com/dn9uy3n/Check-WP-CVE-2020-35489

CVE-2020-29583

Publish Date 22/12/2020

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges.

Links

https://www.zyxel.com/support/CVE-2020-29583.shtml

https://www.eyecontrol.nl/blog/undocumented-user-account-in-zyxel-products.html

CVE-2020-35606

Publish Date 21/12/2020

Exploited Yes

CVSSv3 Rate 8.8 HIGH

Description

Arbitrary command execution can occur in Webmin through 1.962. Any user authorized for the Package Updates module can execute arbitrary commands with root privileges via vectors involving %0A and %0C.

Links

https://www.exploit-db.com/exploits/49318

CVE-2020-1971

Publish Date 08/12/2020

Exploited No

CVSSv3 Rate 5.9 MEDIUM

Description

OpenSSL 1.1 has a remote denial of service (DoS) vulnerability because of NULL point reference issue.

Links

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=f960d81215ebf3f65e03d4d5d857fb9b666d6920

CVE-2020-29492

Publish Date 21/12/2020

Exploited Yes

CVSSv3 Rate 10.0 CRITICAL

Description

Dell Wyse ThinOS 8.6 and prior versions contain an insecure default configuration vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to access the writable file and manipulate the configuration of any target specific station.

Links

https://www.dell.com/support/kbdoc/cs-cz/000180768/dsa-2020-281

https://www.cybermdx.com/vulnerability-research-disclosures/dell-wyse-thin-client-vulnerability

CVE-2020-25179

Publish Date 09/12/2020

Exploited No

CVSSv3 Rate 9.8 CRITICAL

Description

GE Healthcare Imaging and Ultrasound Products may allow specific credentials to be exposed during transport over the network.

Links

https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01

CVE-2020-17141

Publish Date 09/12/2020

Exploited Yes

CVSSv3 Rate 8.4 HIGH

Description

Microsoft Exchange Server has remote code execution allows remote attackers to disclose information on affected installations of Exchange Server. Authentication is required to exploit this vulnerability.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17140

https://srcincite.io/advisories/src-2020-0031/