Vulnerability Digest

August 2020

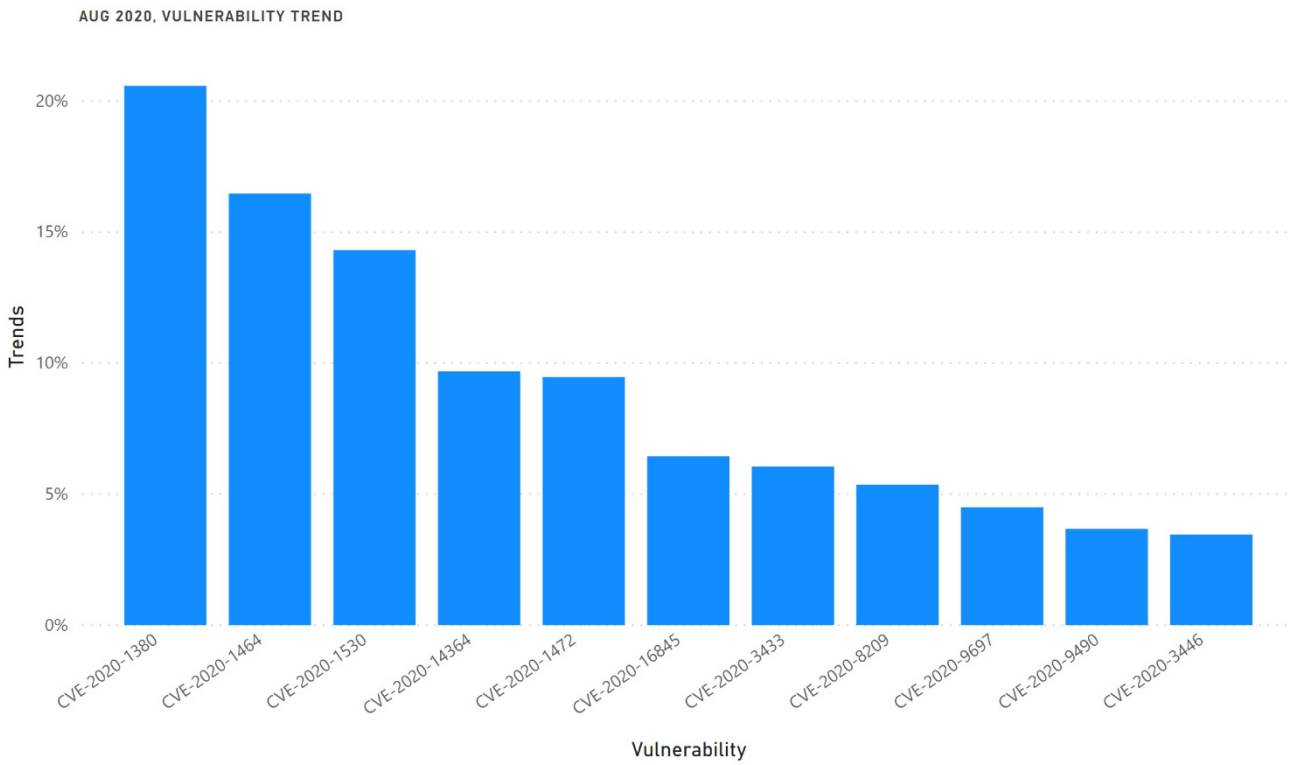
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

Papendrecht 318 3351, 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 August 2020, we see that the information security community pays more attention, again, to Microsoft published vulnerabilities as CVE-2020-1380 which is a vulnerability in Internet Explorer scripting engine caused a remote code execution. This vulnerability gained almost 20% of overall August trends.

Other important August vulnerability is the QEMU which leads to VM escape and impact the host.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2020-1380	IE Scripting Engine Memory Corruption	17/08/2020	Yes	20%
CVE-2020-1464	Windows Spoofing Vulnerability	17/08/2020	Yes	16%
CVE-2020-1530	Elevation of Privilege Windows Remote Access	17/08/2020	Yes	14%
CVE-2020-14364	QEMU VM Escape Vulnerability	24/08/2020	Yes	10%
CVE-2020-1472	Privilege Escalation in Windows Netlogon	17/08/2020	No	10%
CVE-2020-16845	Infinite Read Loop in Go	06/08/2020	No	7%
CVE-2020-3433	DLL Hijacking in Cisco AnyConnect Client	17/08/2020	No	6%
CVE-2020-8209	Arbitrary File Reads in Citrix XenMobile Server	17/08/2020	No	5%
CVE-2020-9697	Memory Read in Adobe Acrobat Reader	19/08/2020	Yes	5%
CVE-2020-9490	DoS in Apache 2	07/08/2020	Yes	4%
CVE-2020-3446	Default Credentials in Cisco vWAAS	19/08/2020	No	3%

*Trends value is rounded.

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

CVE-2020-1380

Publish Date 17/08/2020

Exploited Yes

CVSSv3 Rate 7.5 HIGH

Description

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380

https://www.trendmicro.com/en_us/research/20/h/cve-2020-1380-analysis-of-recently-fixed-ie-zero-day.html

CVE-2020-1464

Publish Date 17/08/2020

Exploited Yes

CVSSv3 Rate 5.5 MEDIUM

Description

A spoofing vulnerability exists when Windows incorrectly validates file signatures. An attacker who successfully exploited this vulnerability could bypass security features and load improperly signed files.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1464

https://medium.com/@TalBeerySec/glueball-the-story-of-cve-2020-1464-50091a1f98bd

https://mp.weixin.qq.com/s/CRdDJeen-Zqc0RCnMr4kzQ

CVE-2020-1530

Publish Date 17/08/2020

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1530

https://symeonp.github.io/2020/12/08/phonebook-uaf-analysis.html

CVE-2020-14364

Publish Date 24/08/2020

Exploited Yes

CVSSv3 Rate 9.3 CRITICAL

Description

The vulnerability exists in the Qemu USB module, which can cause out-of-bounds reading and writing, and thus realize virtual machine escape.

Links

https://xenbits.xen.org/xsa/advisory-335.html

https://www.openwall.com/lists/oss-security/2020/08/24/3

https://meterpreter.org/cve-2020-14364/

CVE-2020-1472

Publish Date 17/08/2020

Exploited No

CVSSv3 Rate 10.0 CRITICAL

Description

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

CVE-2020-16845

Publish Date 06/08/2020

Exploited No

CVSSv3 Rate 7.5 HIGH

Description

Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary via invalid inputs.

Links

https://github.com/golang/go/issues/40618

CVE-2020-3433

Publish Date 17/08/2020

Exploited No

CVSSv3 Rate 7.8 HIGH

Description

A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.

Links

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW

CVE-2020-8209

Publish Date 17/08/2020

Exploited No

CVSSv3 Rate 7.5 HIGH

Description

Improper access control in Citrix XenMobile Server 10.12 before RP2, Citrix XenMobile Server 10.11 before RP4, Citrix XenMobile Server 10.10 before RP6 and Citrix XenMobile Server before 10.9 RP5 and leads to the ability to read arbitrary files.

Links

https://support.citrix.com/article/CTX277457

CVE-2020-9697

Publish Date 19/08/2020

Exploited Yes

CVSSv3 Rate 5.5 MEDIUM

Description

Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a disclosure of sensitive data vulnerability. Successful exploitation could lead to memory leak.

Links

https://helpx.adobe.com/security/products/acrobat/apsb20-48.html

https://twitter.com/thezdi/status/1293568647043190784

CVE-2020-9490

Publish Date 07/08/2020

Exploited Yes

CVSSv3 Rate 7.5 HIGH

Description

Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards.

Links

https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2020-9490

https://twitter.com/wugeej/status/1298464906652475395

CVE-2020-3446

Publish Date 19/08/2020

Exploited No

CVSSv3 Rate 9.8 CRITICAL

Description

Default account vulnerability in Cisco Virtual Wide Area Application Services (vWAAS) with Cisco Enterprise NFV Infrastructure Software (NFVIS)-bundled images for Cisco ENCS 5400-W Series and CSP 5000-W Series appliances could allow an unauthenticated, remote attacker to log into the NFVIS CLI of an affected device by using accounts that have a default, static password.

Links

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-waas-encsw-cspw-cred-hZzL29A7