Vulnerability Digest
April 2020

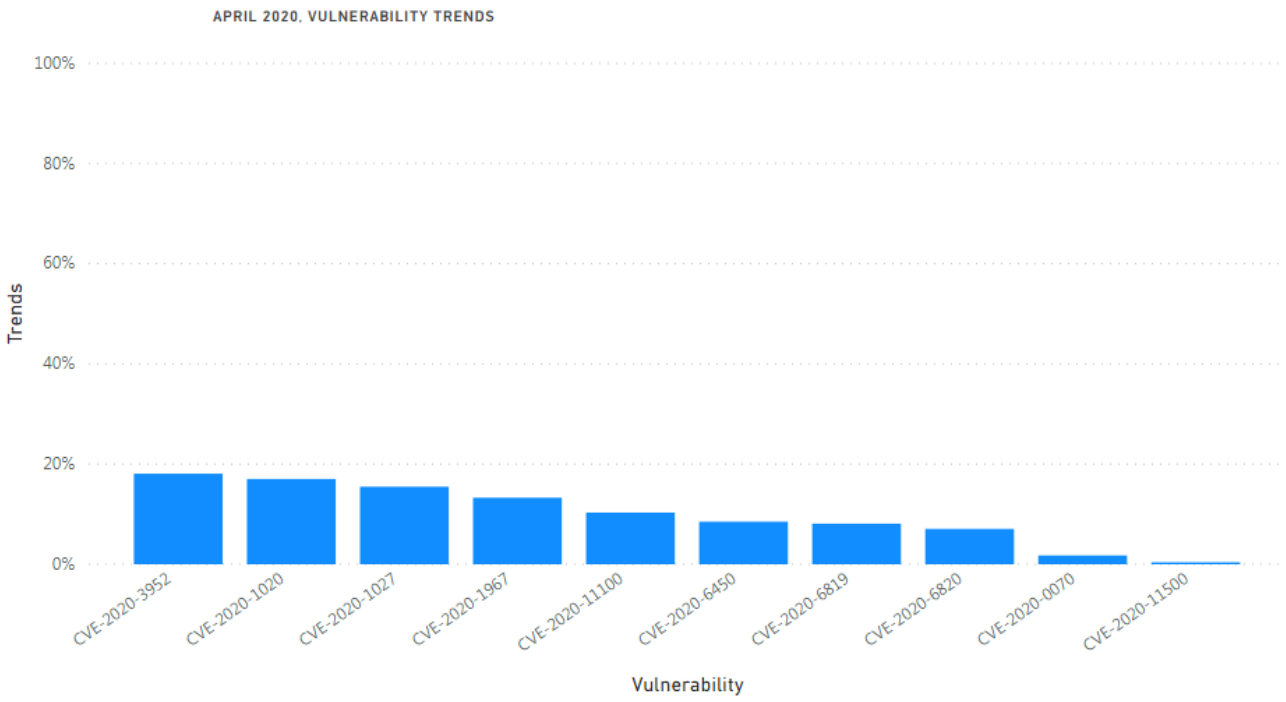
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

Papendrecht 318 3351, Netherlands | info@scantitan.com

SUMMARY

This report shows 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 April 2020, a new critical and exploitable vulnerability in VMware vCenter vmdir (CVE-2020-3952) gained the most attraction of cyber security communities. This vulnerability has almost of 20% of overall April trends.

The next in line is Windows Type Manager RCE and Kernel Elevation vulnerabilities (CVE-2020-1020 and CVE-2020-1027) which were published in Microsoft April patch Tuesday.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2020-3952	VMware vCenter vmdir access control bypass	10/04/2020	Yes	18%
CVE-2020-1020	Windows Type Manager RCE	15/04/2020	Yes	17%
CVE-2020-1027	Windows kernel elevation	15/04/2020	Yes	15%
CVE-2020-1967	OpenSSL DoS	21/04/2020	Yes	13%
CVE-2020-11100	HA Proxy out of bound writes/RCE	01/04/2020	Yes	10%
CVE-2020-6450	Chrome WebAudio use after free	07/04/2020	No	9%
CVE-2020-6819	Firefox use after free	24/04/2020	Yes	8%
CVE-2020-6820	Firefox use after free	24/04/2020	Yes	8%
CVE-2020-0070	Android out-of-Bound Write/RCE	06/04/2020	Yes	2%
CVE-2020-11500	Zoom weak encryption	17/04/2020	Yes	1%

*Trends value is rounded.

CVE-2020-3952

Publish Date 10/04/2020
Exploited Yes
CVSSv3 Rate 9.8 CRITICAL

Description
There is a bug in VMware vCenter vmdir component that allows an attacker to add administrator accounts without restriction and bypassing the access control.

Links
https://www.vmware.com/security/advisories/VMSA-2020-0006
https://www.guardicore.com/2020/04/pwning-vmware-vcenter-cve-2020-3952/

CVE-2020-1020

Publish Date 15/04/2020
Exploited Yes
CVSSv3 Rate 7.8 HIGH

Description
A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'.

Links
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020
https://mp.weixin.qq.com/s/RvTZWvcXiXsI7xB6L9RWIg

CVE-2020-1027

Publish Date 15/04/2020
Exploited Yes
CVSSv3 Rate 7.8 HIGH

Description
An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'.

Links
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1027

CVE-2020-1967

Publish Date 21/04/2020
Exploited Yes
CVSSv3 Rate 7.8 HIGH

Description
Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension.

Links
https://www.openssl.org/news/secadv/20200421.txt
https://github.com/irsl/CVE-2020-1967

CVE-2020-11100

Publish Date 01/04/2020
Exploited Yes
CVSSv3 Rate 8.8 HIGH

Description
In hpack_dht_insert in hpack-tbl.c in the HPACK decoder in HAProxy 1.8 through 2.x before 2.1.4, a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing remote code execution.

Links
https://www.haproxy.org/download/2.1/src/CHANGELOG
https://bugs.chromium.org/p/project-zero/issues/detail?id=2023

CVE-2020-6450

Publish Date 07/04/2020
Exploited No
CVSSv3 Rate 8.8 HIGH

Description
Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

Links
https://chromereleases.googleblog.com/2020/03/stable-channel-update-for-desktop_31.html

CVE-2020-6819

Publish Date 24/04/2020
Exploited Yes
CVSSv3 Rate 8.8 HIGH

Description
Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.

Links
https://www.mozilla.org/security/advisories/mfsa2020-11/

CVE-2020-6820

Publish Date 24/04/2020
Exploited Yes
CVSSv3 Rate 8.8 HIGH

Description
Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.

Links
https://source.android.com/security/bulletin/2020-04-01

CVE-2020-0070

Publish Date 06/04/2020
Exploited Yes
CVSSv3 Rate 9.8 CRITICAL

Description
In rw_t2t_update_lock_attributes of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.

Links
https://source.android.com/security/bulletin/2020-04-01
https://securitylab.github.com/advisories/GHSL-2020-010-aosp

CVE-2020-11500

Publish Date 17/04/2020
Exploited Yes
CVSSv3 Rate 7.5 HIGH

Description
Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.

Links
https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/