Vulnerability Digest

June 2020

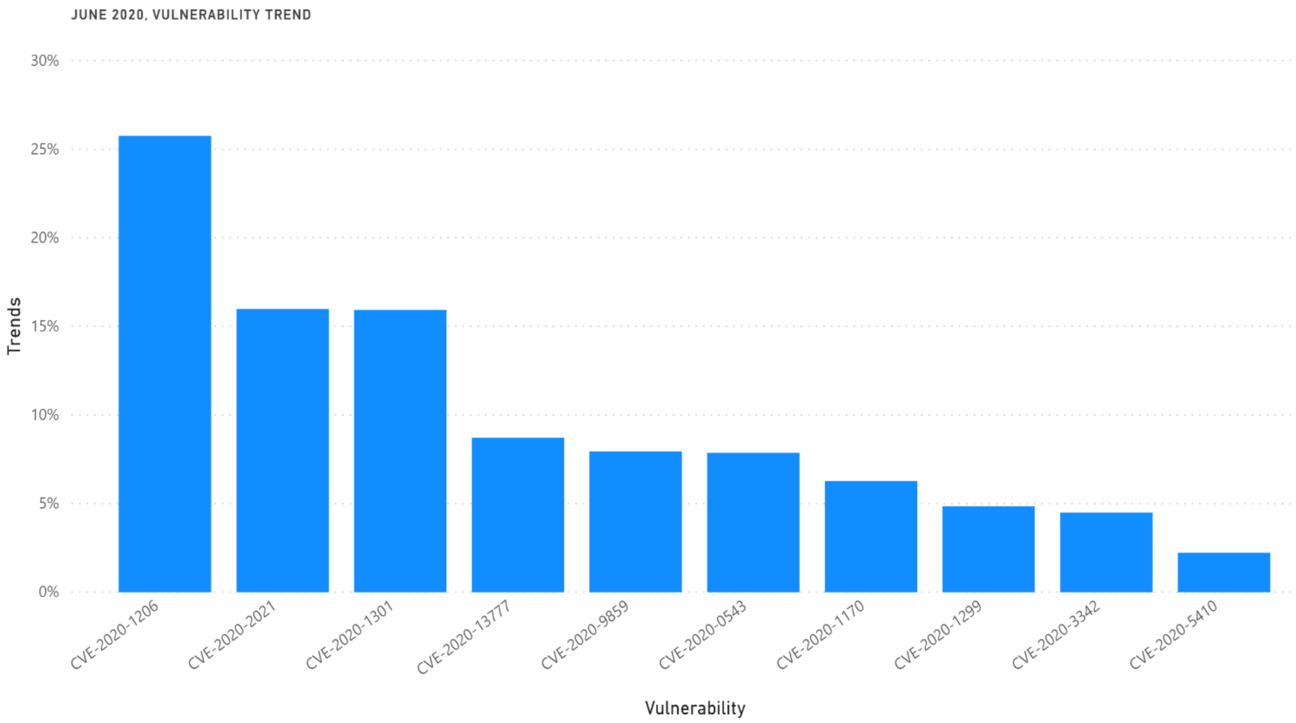
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

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 June 2020, we see that the information security community pays more attention, again, to Microsoft published vulnerabilities as CVE-2020-1206, dubbed as SMBleed, gained most trends. This vulnerability gained almost 25% of overall May trends.

The next in line is the critical, not yet exploitable, PaloAlto, CVE-2020-2021, authentication bypass in SAML. Although it is published at the end of June, it got more security community attentions.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2020-1206	SMBleed Information Disclosure in SMBv3	09/06/2020	Yes	25%
CVE-2020-2021	PaloAlto Firewall Authentication Bypass	29/06/2020	No	16%
CVE-2020-1301	SMBLost Remote Code Execution in SMBv1	09/06/2020	Yes	16%
CVE-2020-13777	GnuTLS Insecure Session Tickets (TLS 1.2 & 1.3)	04/06/2020	Yes	9%
CVE-2020-9859	Privilege Escalation in Apple iOS and MacOS	05/06/2020	Yes	8%
CVE-2020-0543	CrossTalk Information Disclosure in Intel CPUs	09/06/2020	Yes	8%
CVE-2020-1170	Elevation of Privilege in Windows Defender	09/06/2020	Yes	7%
CVE-2020-3342	RCE in Webex Meetings Desktop App	17/06/2020	No	5%
CVE-2020-1299	LNK Remote Code Execution in Windows	09/06/2020	Yes	3%
CVE-2020-5410	Directory Traversal in Spring Cloud Config	02/06/2020	Yes	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-2020-1206

Publish Date	09/06/2020
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

SMBleed is an information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1206

https://github.com/ZecOps/CVE-2020-1206-POC

https://packetstormsecurity.com/files/158053/SMBleed-Uninitialized-Kernel-Memory-Read-Proof-Of-Concept.html

CVE-2020-2021

Publish Date	29/06/2020
Exploited	No
CVSSv3 Rate	10 CRITICAL

Description

If SAML is enabled, PAN-OS is vulnerable to authentication bypass in SAML implementation in Paloalto firewalls operating system (PAN-OS). This vulnerability allows an attacker to access protected resources in the firewall without authentication.

Links

https://security.paloaltonetworks.com/CVE-2020-2021

CVE-2020-1301

Publish Date	09/06/2020
Exploited	Yes
CVSSv3 Rate	8.8 HIGH

Description

SMBleed is an information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Information Disclosure Vulnerability'.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1301

https://github.com/shubham0d/CVE-2020-1301

CVE-2020-13777

Publish Date	04/06/2020
Exploited	Yes
CVSSv3 Rate	7.4 HIGH

Description

GnuTLS library, widely used for TLS implementation, has a vulnerability in constructing an insecure session ticket encryption keys, allowing a MitM attacker to bypass authentication in TLS 1.3 and recover previous conversations in TLS 1.2.

Links

https://gnutls.org/security-new.html#GNUTLS-SA-2020-06-03
https://github.com/shigeki/challenge_CVE-2020-13777
https://github.com/0xxon/cve-2020-13777

CVE-2020-9859

Publish Date	05/06/2020
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

Privilege escalation vulnerability due to a memory consumption issue which was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6.

An application may be able to execute arbitrary code with kernel privileges and this vulnerability was used by “unc0ver” jailbreak tool.

Links

https://support.apple.com/en-us/HT211214

CVE-2020-0543

Publish Date	09/06/2020
Exploited	No
CVSSv3 Rate	5.5 MEDIUM

Description

CrossTalk vulnerability is a side-channel vulnerability due to incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

Links

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00320.html

CVE-2020-1170

Publish Date	09/06/2020
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1170

https://itm4n.github.io/cve-2020-1170-windows-defender-eop/

CVE-2020-3342

Publish Date	17/06/2020
Exploited	No
CVSSv3 Rate	8.8 HIGH

Description

A vulnerability in the software update feature of Cisco Webex Meetings Desktop App for Mac could allow an unauthenticated, remote attacker to execute arbitrary code on an affected system. The vulnerability is due to improper validation of cryptographic protections on files that are downloaded by the application as part of a software update.

Links

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-mac-X7vp65BL

CVE-2020-1299

Publish Date	09/06/2020
Exploited	Yes
CVSSv3 Rate	7.8 HIGH

Description

LNK remote code execution exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1299

https://blog.vincss.net/2020/06/cve49-microsoft-windows-lnk-remote-code-execution-vuln-cve-2020-1299-eng.html

CVE-2020-5410

Publish Date	02/06/2020
Exploited	No
CVSSv3 Rate	7.5 HIGH

Description

Spring Cloud Config allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack.

Links

https://tanzu.vmware.com/security/cve-2020-5410