Vulnerability Digest

March 2021

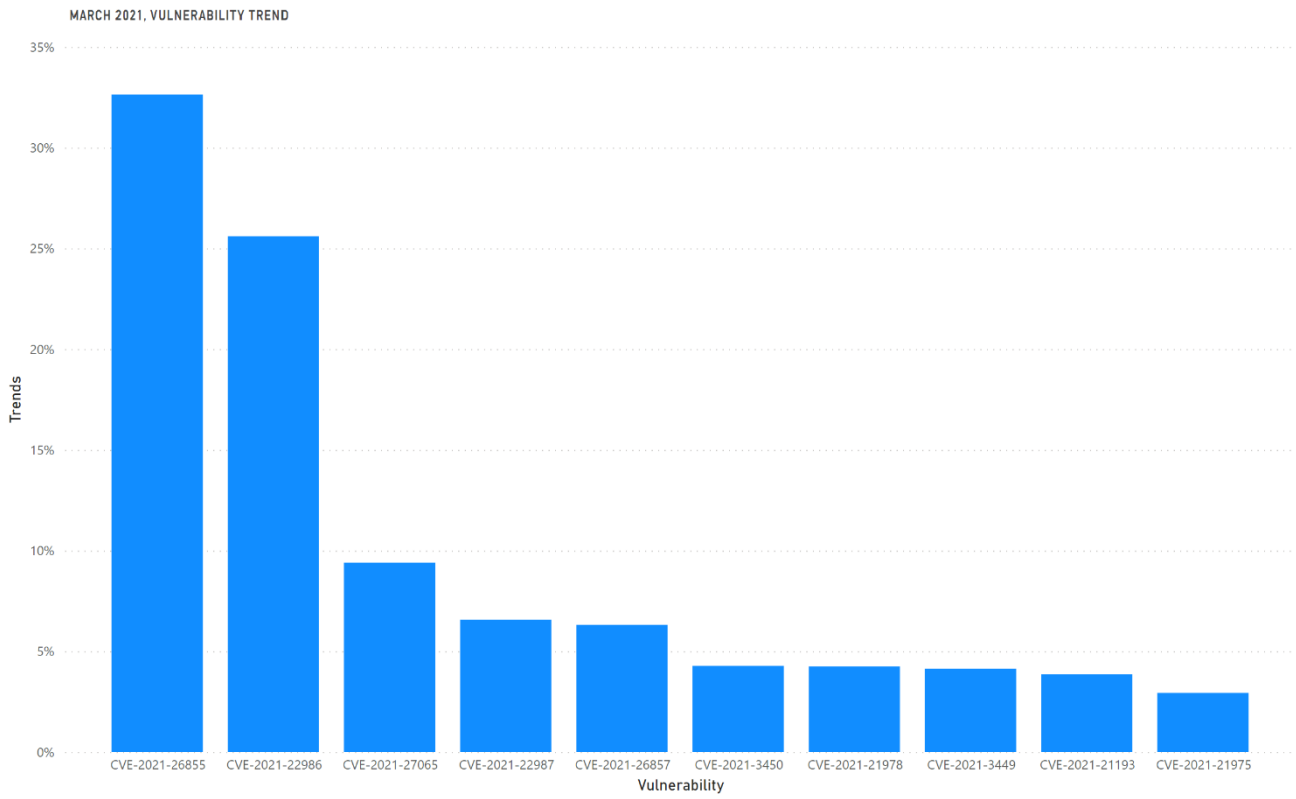
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

2563AP 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.



March 2021 was the month of Microsoft Exchange where most of the trends and attacks were related to the critical RCE and SSRF in Microsoft Exchange. Those vulnerabilities got realized after discovering attacks weaponizing them to target official and government organizations.

Other critical and important vulnerabilities were discovered in F5 BIG-IP, OpenSSL, and VMware.

The following table shows the summary of the trends.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2021-26855	SSRF in Microsoft Exchange	02/03/2021	Yes	32%
CVE-2021-22986	Remote Code Execution in F5 BIG-IP API	10/03/2021	Yes	26%
CVE-2021-27065	Arbitrary file write in Microsoft Exchange	02/03/2021	Yes	10%
CVE-2021-22987	Remote Code Execution in F5 BIG-IP	10/03/2021	No	7%
CVE-2021-26857	Remote Code Execution in Microsoft Exchange	02/03/2021	Yes	6%
CVE-2021-3450	Certificate Validation Bypass in OpenSSL	23/03/2021	No	4%
CVE-2021-21978	Remote Code Execution in VMware Planner	03/03/2021	Yes	4%
CVE-2021-3449	Denial of Service in OpenSSL	23/03/2021	Yes	4%
CVE-2021-21193	Code Execution in Google Chrome	12/03/2021	Yes	4%
CVE-2021-21975	SSRF in VMware vRealize	30/03/2021	Yes	3%

*Trends value is rounded.

Next pages show the details for each vulnerability.

CVE-2021-26855

Publish Date 02/03/2021

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

Remote code execution on Microsoft Exchange Server through server-side-request-forgery (SSRF) vulnerability which allows an unauthenticated attacker to exploit this vulnerability and execute arbitrary codes.

Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855

https://packetstormsecurity.com/files/161846/Microsoft-Exchange-2019-SSRF-Arbitrary-File-Write.html

CVE-2021-22986

Publish Date 10/03/2021

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

F5 iControl REST interface has remote code execution vulnerability through the BIG-IP management interface and self IP addresses, which allow an attacker to execute arbitrary system commands, create or delete files, and disable services.

Links

https://support.f5.com/csp/article/K03009991

https://packetstormsecurity.com/files/162066/F5-BIG-IP-16.0.x-Remote-Code-Execution.html

CVE-2021-27065

Publish Date 02/03/2021

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

Arbitrary files write on any path on Exchange server. This vulnerability is used as a post-authentication exploit mainly after exploiting CVE-2021-26855.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27065

http://packetstormsecurity.com/files/161938/Microsoft-Exchange-ProxyLogon-Remote-Code-Execution.html

CVE-2021-22987

Publish Date 10/03/2021

Exploited No

CVSSv3 Rate 9.8 CRITICAL

Description

F5 BIG-IP when running in Appliance mode, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages.

Links

https://support.f5.com/csp/article/K18132488

CVE-2021-26857

Publish Date 02/03/2021

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

Deserialization vulnerability exists in Exchange Server's Unified Messaging (voicemail) service. This vulnerability is used as a post-authentication exploit mainly after exploiting CVE-2021-26855.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857

https://attackerkb.com/topics/hx6O9H590s/cve-2021-26857

CVE-2021-3450

Publish Date 23/03/2021

Exploited No

CVSSv3 Rate 7.4 HIGH

Description

OpenSSL has a vulnerability that prevents applications from detecting and rejecting TLS certificates that aren't digitally signed by a browser-trusted certificate authority.

Links

https://www.openssl.org/news/secadv/20210325.txt

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2a40b7bc7b94dd7de897a74571e7024f0cf0d63b

CVE-2021-21978

Publish Date 03/03/2021

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

VMware View Planner contains a remote code execution vulnerability. Improper input validation and lack of authorization leading to arbitrary file upload in logupload web application by any unauthenticated user with network access.

Links

https://www.vmware.com/security/advisories/VMSA-2021-0003.html

https://packetstormsecurity.com/files/161879/VMware-View-Planner-4.6-Remote-Code-Execution.html

CVE-2021-3449

Publish Date 23/03/2021

Exploited Yes

CVSSv3 Rate 5.9 MEDIUM

Description

OpenSSL has a denial of service vulnerability that can be exploited by any client if sent a maliciously crafted renegotiation ClientHello message.

Links

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fb9fa6b51defd48157eeb207f52181f735d96148

https://github.com/terorie/cve-2021-3449

CVE-2021-21193

Publish Date 12/03/2021

Exploited Yes

CVSSv3 Rate 8.8 HIGH

Description

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

Links

https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html

CVE-2021-21975

Publish Date 30/03/2021

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

Server Side Request Forgery in vRealize Operations Manager API may allow a malicious actor with network access to exploit this vulnerability and compromise administrative credentials.

Links

https://www.vmware.com/security/advisories/VMSA-2021-0004.html

https://github.com/Henry4E36/VMWare-vRealize-SSRF