Vulnerability Digest
February 2021

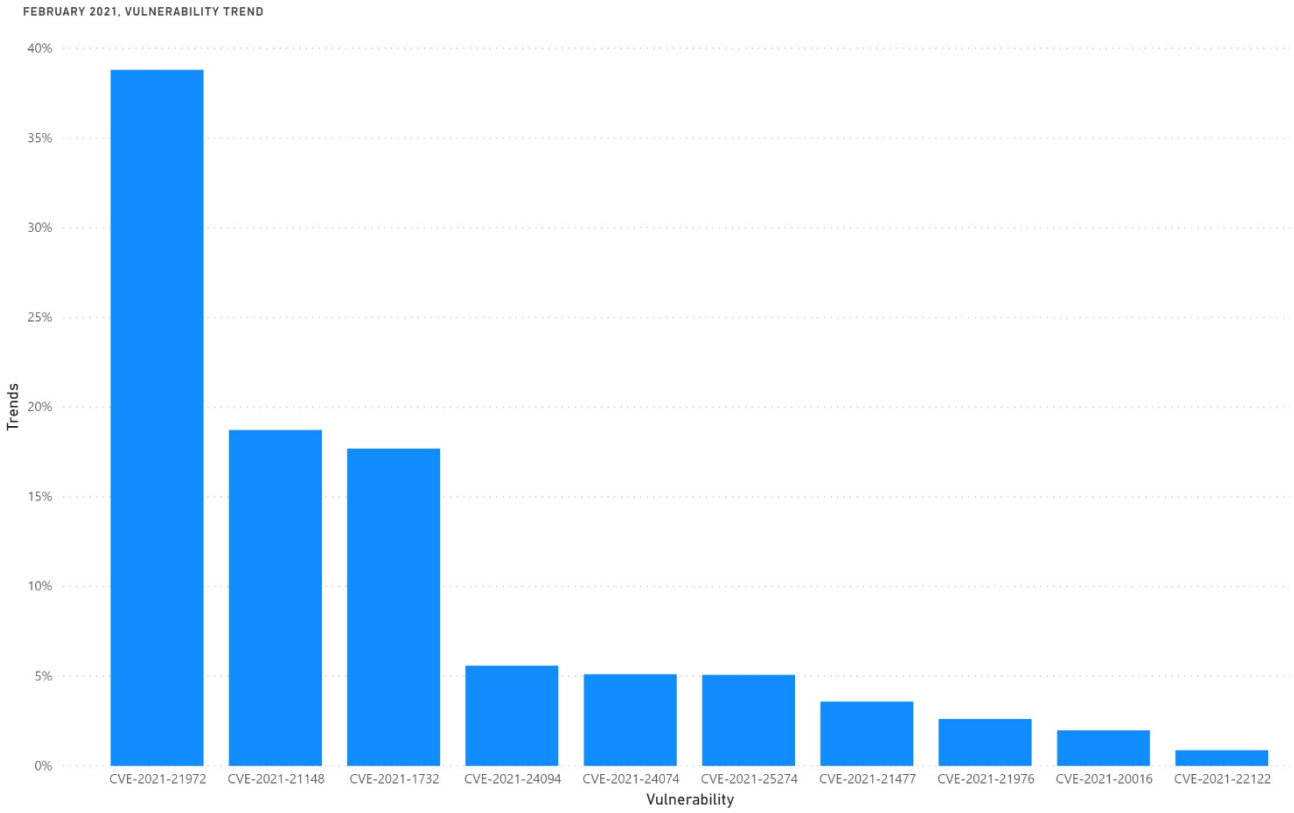
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

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.



Feb 2021 had variety of vulnerabilities discovered and made public with most of them are related to remote code execution. The vulnerability with the most interactions is a remote code execution exists in vCenter, CVE-2021-21972, which is still under active exploitation.

Other critical and important vulnerabilities were discovered in Windows, SolarWinds, SAP, SonicWall and FortiWeb.

The following table shows the summary of the trends.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2021-21972	Remote Code Execution in vCenter/vSphere	23/02/2021	Yes	38%
CVE-2021-21148	Heap overflow in Chrome V8 engine	04/02/2021	Yes	19%
CVE-2021-1732	Privilege Escalation in Windows kernel	09/02/2021	Yes	17%
CVE-2021-24094	Remote Code Execution in Windows IPv6	09/02/2021	No	6%
CVE-2021-24074	Remote Code Execution in Windows TCP/IP IPv4	09/02/2021	No	5%
CVE-2021-25274	Remote Code Execution in SolarWinds Orion	03/02/2021	Yes	5%
CVE-2021-21477	Remote Code Execution in SAP Commerce Cloud	09/02/2021	No	4%
CVE-2021-21976	Command Injection in vSphere Replication	11/02/2021	No	3%
CVE-2021-20016	SQL Injection in SonicWall SSL VPN	03/02/2021	Yes	2%
CVE-2021-22122	Reflective XSS in FortiWeb GUI	04/02/2021	Yes	1%

*Trends value is rounded.

Next pages show the details for each vulnerability.

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

CVE-2021-21972

Publish Date 23/02/2021

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

Remote code execution vulnerability exists in VMware vCenter/vSphere that allows an unauthenticated attacker to remotely execute code on the VMware hypervisor. Where any attacker can upload a code and execute it to control VMware hypervisor.

Links

https://www.vmware.com/security/advisories/VMSA-2021-0002.html

https://swarm.ptsecurity.com/unauth-rce-vmware/

CVE-2021-21148

Publish Date 04/02/2021

Exploited Yes

CVSSv3 Rate 8.5 HIGH

Description

Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.150 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

Links

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html

CVE-2021-1732

Publish Date 09/02/2021

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

Windows Kernel privilege escalation vulnerability exists in Windows 10 and Windows Server 2019.

Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1732

https://ti.dbappsecurity.com.cn/blog/index.php/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/

CVE-2021-24094

Publish Date 09/02/2021

Exploited No

CVSSv3 Rate 9.8 CRITICAL

Description

Remote code execution vulnerability exists in all Windows IPv6 implementation. This affects IPv6 link-local addresses as well.

Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-24094

https://msrc-blog.microsoft.com/2021/02/09/multiple-security-updates-affecting-tcp-ip/

CVE-2021-24074

Publish Date 09/02/2021

Exploited No

CVSSv3 Rate 9.8 CRITICAL

Description

Remote code execution vulnerability exists in Windows IPv4 TCP/IP.

Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-24074

https://msrc-blog.microsoft.com/2021/02/09/multiple-security-updates-affecting-tcp-ip/

CVE-2021-25274

Publish Date 03/02/2021

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

Remote code execution vulnerability exists in SolarWinds Orion platform as it does not add security on the private queues. Thus, any attacker can connect and send codes to be executed.

Links

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/full-system-control-with-new-solarwinds-orion-based-and-serv-u-ftp-vulnerabilities/

https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/release_notes/orion_platform_2020-2-4_release_notes.htm

CVE-2021-21477

Publish Date 09/02/2021

Exploited No

CVSSv3 Rate 9.8 CRITICAL

Description

Remote code execution vulnerability exists in SAP Commerce Cloud, enables certain users with required privileges to edit drools rules and inject arbitrary or malicious code.

Links

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=568460543

CVE-2021-21976

Publish Date 11/02/2021

Exploited No

CVSSv3 Rate 7.5 HIGH

Description

Command injection vulnerability exists in vSphere Replication where an authenticated admin can inject and execute any command.

Links

https://www.vmware.com/security/advisories/VMSA-2021-0001.html

CVE-2021-20016

Publish Date 03/02/2021

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information.

Links

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

CVE-2021-22122

Publish Date 04/02/2021

Exploited Yes

CVSSv3 Rate 4.2 MEDIUM

Description

A Cross Site Scriptting (XSS) vulnerability exists in FortiWeb GUI may allow an unauthenticated, remote attacker to perform a reflected cross site scripting attack (XSS) by injecting malicious payload in different vulnerable API end-points.

Links

https://fortiguard.com/advisory/FG-IR-20-122

https://twitter.com/ptswarm/status/1357316793753362433

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