Vulnerability Digest

October 2020

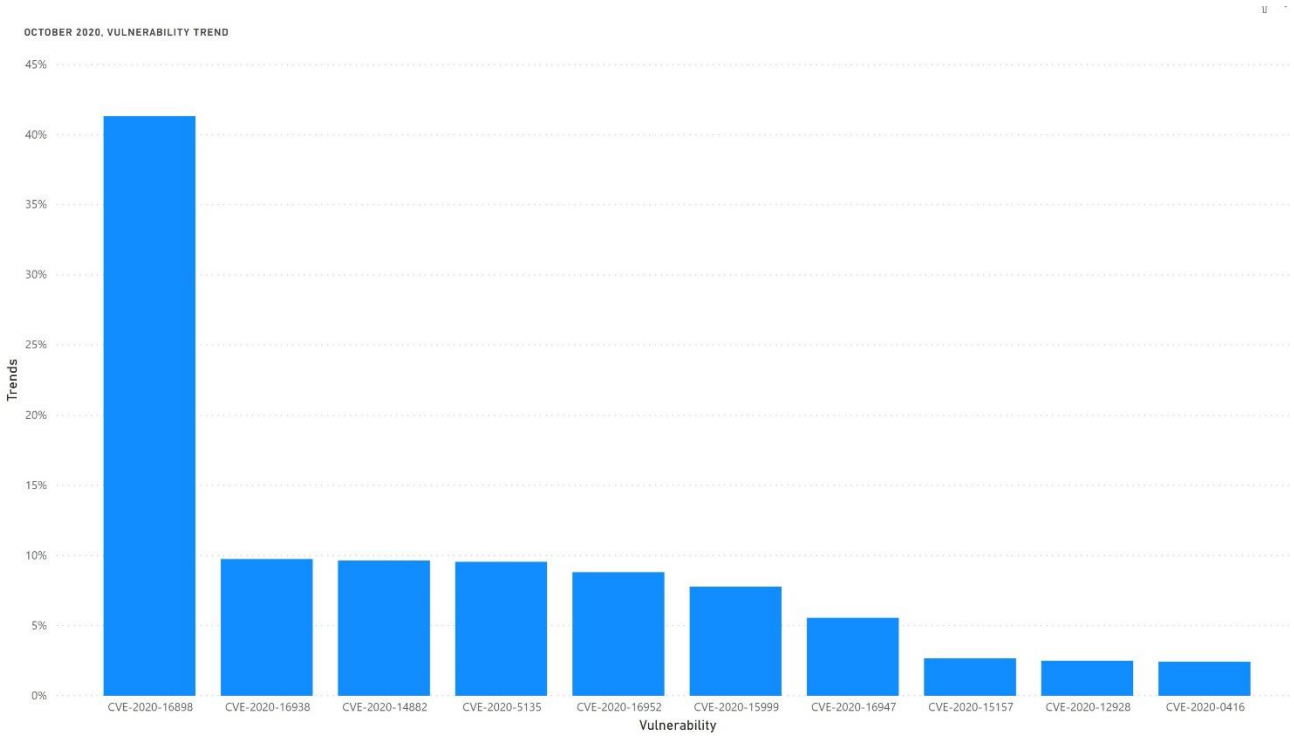
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

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.



In October 2020, we see cyber security community responded more to Microsoft vulnerabilities. Especially. the Bad Neighbor or Ping of Death Redux where it gained 40% of overall October trends.

Other important vulnerabilities have been reported as trends. That includes Oracle Web Logic RCE and Heap overflow in Google Chrome.

The following table shows the summary of the trends.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2020-16898	Bad Neighbour / Ping of Death Redux	16/10/2020	Yes	41%
CVE-2020-16938	Privilege Escalation in Windows	16/10/2020	Yes	10%
CVE-2020-14882	RCE in Oracle Web Logic	21/10/2020	Yes	10%
CVE-2020-5135	DoS in SonicWall	12/10/2020	No	10%
CVE-2020-16952	RCE in Microsoft Sharepoint	16/10/2020	Yes	9%
CVE-2020-15999	Heap Overflow in Chrome Freetype	21/10/2020	Yes	8%
CVE-2020-16947	RCE in Microsoft Outlook Client	16/10/2020	Yes	5%
CVE-2020-12928	Privilege Escalation in AMD Ryzen Master	13/10/2020	Yes	3%
CVE-2020-0416	Privilege Escalation in Android	14/10/2020	No	2%
CVE-2020-15157	Credential Leakage in Containerd	15/10/2020	No	2%

*Trends value is rounded.

Next pages show the details for each vulnerability.

CVE-2020-16898

Publish Date 16/10/2020

Exploited Yes

CVSSv3 Rate 8.8 HIGH

Description

A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. This vulnerability known as “Bad Neighbor” / “Ping of Death Redux”.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898

https://blog.quarkslab.com/beware-the-bad-neighbor-analysis-and-poc-of-the-windows-ipv6-router-advertisement-vulnerability-cve-2020-16898.html

CVE-2020-16938

Publish Date 16/10/2020

Exploited Yes

CVSSv3 Rate 5.5 MEDIUM

Description

An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. This vulnerability that allows you to get unrestricted file read capabilities on the entire disk as unprivileged user.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16938

https://github.com/ioncodes/CVE-2020-16938

CVE-2020-14882

Publish Date 21/10/2020

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.

Links

https://www.oracle.com/security-alerts/cpuoct2020.html

https://packetstormsecurity.com/files/159769/Oracle-WebLogic-Server-Remote-Code-Execution.html

CVE-2020-5135

Publish Date 12/10/2020

Exploited No

CVSSv3 Rate 9.8 CRITICAL

Description

A buffer overflow vulnerability in SonicOS allows a remote attacker to cause Denial of Service (DoS) and potentially execute arbitrary code by sending a malicious request to the firewall.

Links

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0010

CVE-2020-16952

Publish Date 16/10/2020

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16952

https://packetstormsecurity.com/files/159612/Microsoft-SharePoint-SSI-ViewState-Remote-Code-Execution.html

CVE-2020-15999

Publish Date 21/10/2020

Exploited Yes

CVSSv3 Rate 5.5 MEDIUM

Description

Heap buffer overflow in Freetype implementation in Google Chrome.

Links

https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html

https://bugs.chromium.org/p/chromium/issues/detail?id=1139963

CVE-2020-16947

Publish Date 16/10/2020

Exploited Yes

CVSSv3 Rate 8.8 HIGH

Description

A remote code execution vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16947

https://github.com/0neb1n/CVE-2020-16947

CVE-2020-12928

Publish Date 13/10/2020

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

A vulnerability in a dynamically loaded AMD driver in AMD Ryzen Master V15 may allow any authenticated user to escalate privileges to NT authority system.

Links

https://www.amd.com/en/corporate/product-security

https://h0mbre.github.io/RyzenMaster_CVE/?fbclid=IwAR0ddvDtjXgR5UIzAk00y8i90YZ39BrayUKNPPBRT0Oivc5Kl7VOSCw6oXQ#

CVE-2020-0416

Publish Date 14/10/2020

Exploited No

CVSSv3 Rate 8.8 HIGH

Description

In multiple settings screens, there are possible tapjacking attacks due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed.

Links

https://source.android.com/security/bulletin/2020-10-01

CVE-2020-15157

Publish Date 15/10/2020

Exploited No

CVSSv3 Rate 6.1 MEDIUM

Description

Containerd can be coerced into leaking credentials during image pull.

Links

https://github.com/containerd/containerd/security/advisories/GHSA-742w-89gc-8m9c