CSW Cyber SecurityWorks

April - 2020

COVID-19 **Cyber Risk in Working Remotely**

Table of Contents

Disclaimer

The views and opinions expressed in this report are based on our experience and do not necessarily reflect the official policy of any of the companies mentioned in this paper. Any content provided in this paper is just an opinion and is not intended to malign any organization, company, product or individual.

Executive Summary

The COVID-19 pandemic has forced the entire world to work from our homes. Working-from-home was a trend on the fringe for a long time but now it has become a new normal. In these circumstances, how safe are we from cyber threats?

For this report series, Cyber Security Works examined variant technology, popular application programs, and technology that are currently being used by companies and organizations.

Most software technology has inherent vulnerabilities; some are known but many are unknown. Most of the COVID-19 lockdowns world over were not planned. It was a quickly executed precautionary measure that went on for weeks and became a perfect opportunity for threat actors to find back doors to breach into applications.

Experts at Cyber Security Works picked popular vendors, applications, and technologies and examined them carefully for vulnerabilities. Each report within these series lists vulnerabilities that have always existed and the number of CVEs that have become weaponized over the years. We also brought popular scanners under our microscope to see how many of these vulnerabilities are being detected.

Lastly, we also provide recommendations and priority to fix these vulnerabilities which would provide the users with a safe and secure environment to work with.

A few takeaways

History of vulnerabilities
Learn about the weaponization trend of vulnerabilities for the past two decades for variant technology and popular vendors.

In-depth study of vulnerabilities
From existing to weaponized vulnerability, know more about technologies that might pose a cyber threat to your organization.

Recommendation & way forward
A prioritized list of vulnerabilities that needs to be fixed and an in-depth study of scan systems that have missed critical vulnerabilities.

Even while we prepared the report, threat actors have been working fast, breaching systems, stealing data, and possibly holding them for ransom. Staying one step ahead of cyber-attacks is a prudent course of action under any circumstances.

Purpose of this report

This is the first in a series of ten reports where we will seek to highlight how vulnerable popular tech stacks are and provide insights into CVEs that went undetected by leading scan solutions. This report focuses on popular tech stacks as a whole and brings you in-depth insights into common CVEs that could be exploited. In the subsequent reports, we will focus exclusively on top technologies and applications that can be weaponized and exploited.

In this report we bring you -

1. **Technology that has more weaponized vulnerabilities**
2. **Identify vulnerabilities that can be triggered remotely**
3. **Rate of weaponization over the last few years**
4. **Prioritizing vulnerabilities based on weaponization**
5. **Highlighting the quanta of exploitable vulnerabilities that go undetected even by top scan solutions**

Introduction

Coronavirus (COVID) Pandemic has brought the world to a stand-still forcing many to work remotely from the safety of their homes.

We are undergoing an unprecedented situation. All around the world, companies have shut their offices and have provided their employees with infrastructure and tech stacks that would enable them to work from home.

Applications and technology that were once used securely within one's office are now accessed from home. While this has enabled the work to go on, it has also made the tech stacks vulnerable to cyber threats. For threat actors, this is a perfect opportunity to breach, steal data, or implant back doors into the organization's application compromising security.

Today, we are looking at a situation where most offices and organizations will be operating from home for a long time therefore people are largely dependent on popular scan systems to help combat cyber threats.

But how reliable are these scan systems? Do you think they are alerting you about all critical vulnerabilities of your system?

Let us find out….

Vulnerable Technologies and your focus area(s)

Most Governments and companies across the world are heavily dependent on technology for getting their business done. They must have implemented most or at least a few of these products and solutions from leading vendors over the past decades. Each of these serves a specific purpose.

For this study, we selected leading vendors from Gartner and Forrester's research. To view the list of all vendors who went under our microscope, please refer to Appendix I.

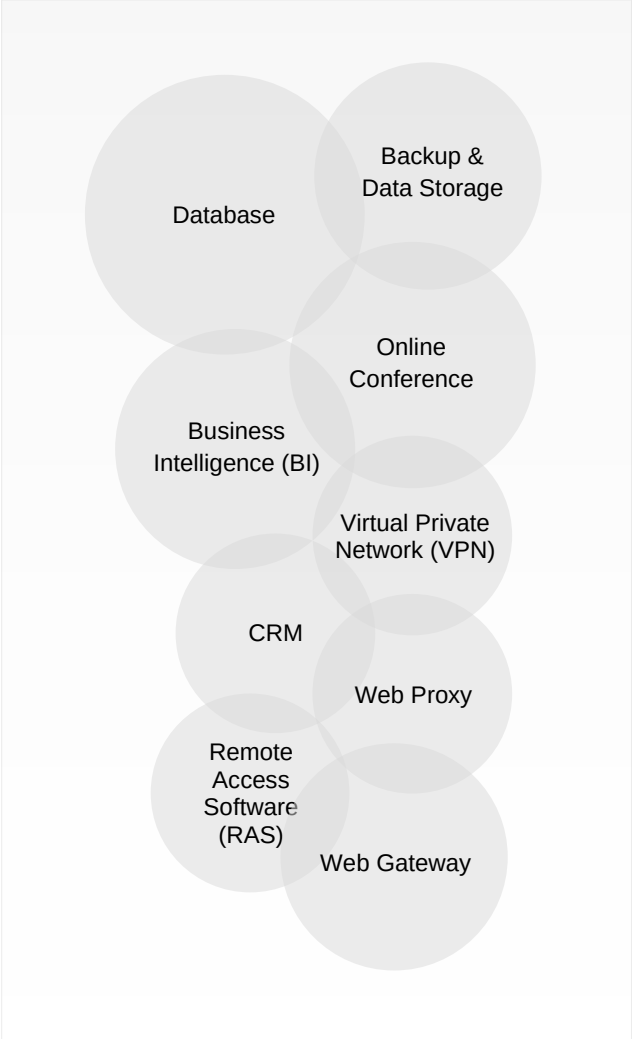

Figure 1: Tech Stacks Covered

An Overview of Vulnerabilities

The tech stacks listed in Figure 1 have been around for a long time and likewise, have a long history of vulnerabilities. The earliest vulnerabilities (CVE) date back to 1999 from databases and backup-storage devices. The first VPN, Remote Access, and Web Proxy vulnerabilities were seen in 2001 and 2002.

We analyzed **4,849** vulnerabilities spanning across all these technologies from 1999 through February of 2020. We further refined the list of vulnerabilities that pose a real risk to an organization. We also highlighted weaponized vulnerabilities for which exploit code already exists.

These vulnerabilities are critical and important to an organization. In general, most vulnerabilities are not weaponized, but our research shows that **546** out of **4,849** CVE entries are being weaponized.

Vulnerabilities by Tech Stacks

These results are interesting when we compare the vulnerability trends seen across all technologies. Figure 2 shows that Database, Online Conference, and Backup & Storage technologies have a large number of vulnerabilities. However, when it comes to weaponization, the count in Database and Backup & Storage is the highest followed by Online Conference, Web Gateways, and VPNs. Figure 3 shows the distribution of vulnerabilities based on the Common Vulnerability Scoring System Version 2 (CVSS 2) assessment. Most number of critical and high vulnerabilities are from Online Conference, Databases, and Backup & Storage technologies.

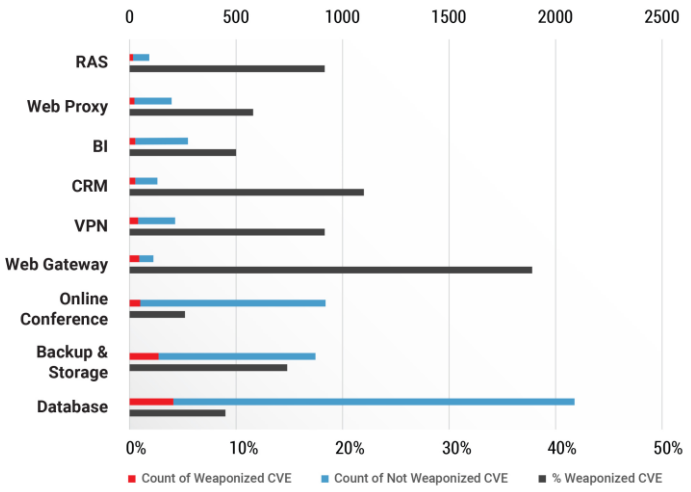

Figure 2: Weaponization of CVEs for Enterprise Technologies

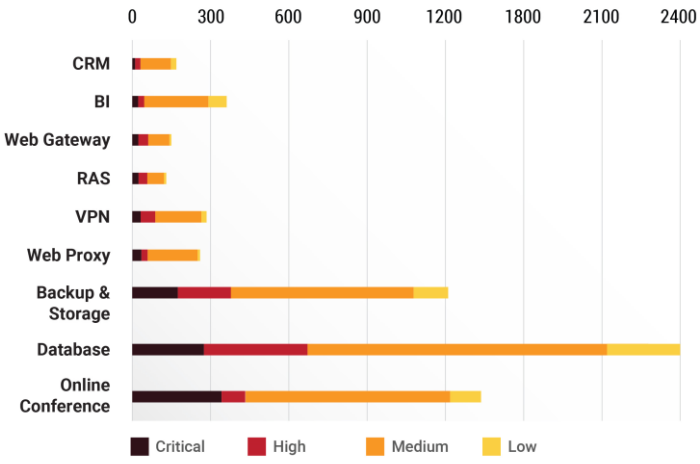

Figure 3: CVE Distribution for Enterprise Technologies (CVSS 2)

Vulnerabilities – Over the years

We next analyzed the dataset by the year to see how the weaponization of vulnerabilities has been changing over the years. Figure 4 shows each year broken by vulnerabilities that were weaponized versus those that were not. Data in 2020 only includes vulnerabilities through the end of February.

Here we can see that weaponization rates have increased considerably since 2015. The number of vulnerabilities discovered has also increased steadily since 2015 with a pronounced spike in 2017.

An Overview of Vulnerabilities (Continued)

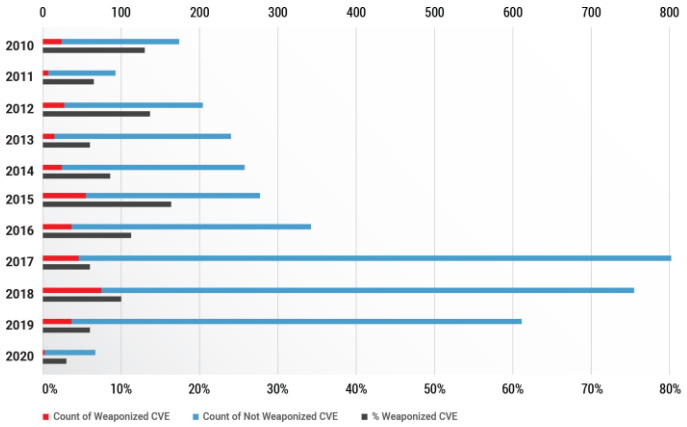

Figure 4: Weaponization of CVEs (2010 -2020)

Vulnerability Prioritization by Weaponization

We further analyzed the vulnerabilities that are of high impact, those that enabled remote code execution (RCE), privilege escalation (PE), and/or an association with a known Ransomware.

We found 201 vulnerabilities enabled remote code execution, **105** vulnerabilities enabled privilege escalation, and **6** vulnerabilities are linked to a known Ransomware. All RCE and PE capable vulnerabilities are weaponized. Figure 1 below shows that security teams should first focus on Ransomware, RCE, and PE related vulnerabilities.

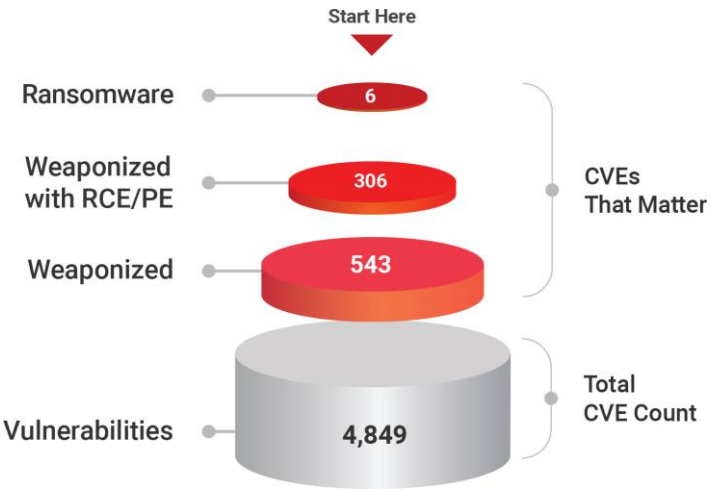

Figure 5: Vulnerabilities prioritization across Enterprise Technologies

Vulnerabilities Missed by Scan Solutions

We analyzed the data further by comparing the CVEs with the plugins from some of the best scan solutions. It is very interesting to learn that the leading scan solutions fail to detect critical and high vulnerabilities that have weaponized exploits in the wild. Table 1 below shows the count of vulnerabilities from 1999 to 2020 that were missed by scanners. Chord diagram (Figure 6) shows the number of vulnerabilities from 2010 to 2020, that was missed by the scanners. To view the list of undetected CVEs, please refer to Appendix II.

	NESSUS	NEXPOSE	QUALYS
VPN	6	12	8
RAS	5	8	5
DATABASE	23	49	32
WEB PROXY	2	5	3
WEB GATEWAY	1	12	3
CRM	5	6	5
BI	4	2	5
BACKUP & DATA STORAGE	44	46	33
ONLINE CONFERENCE	10	22	8
Total	**100**	**162**	**102**

Table 1: Count of Vulnerabilities Missed

Vulnerabilities Undetected by Top Scan Solutions

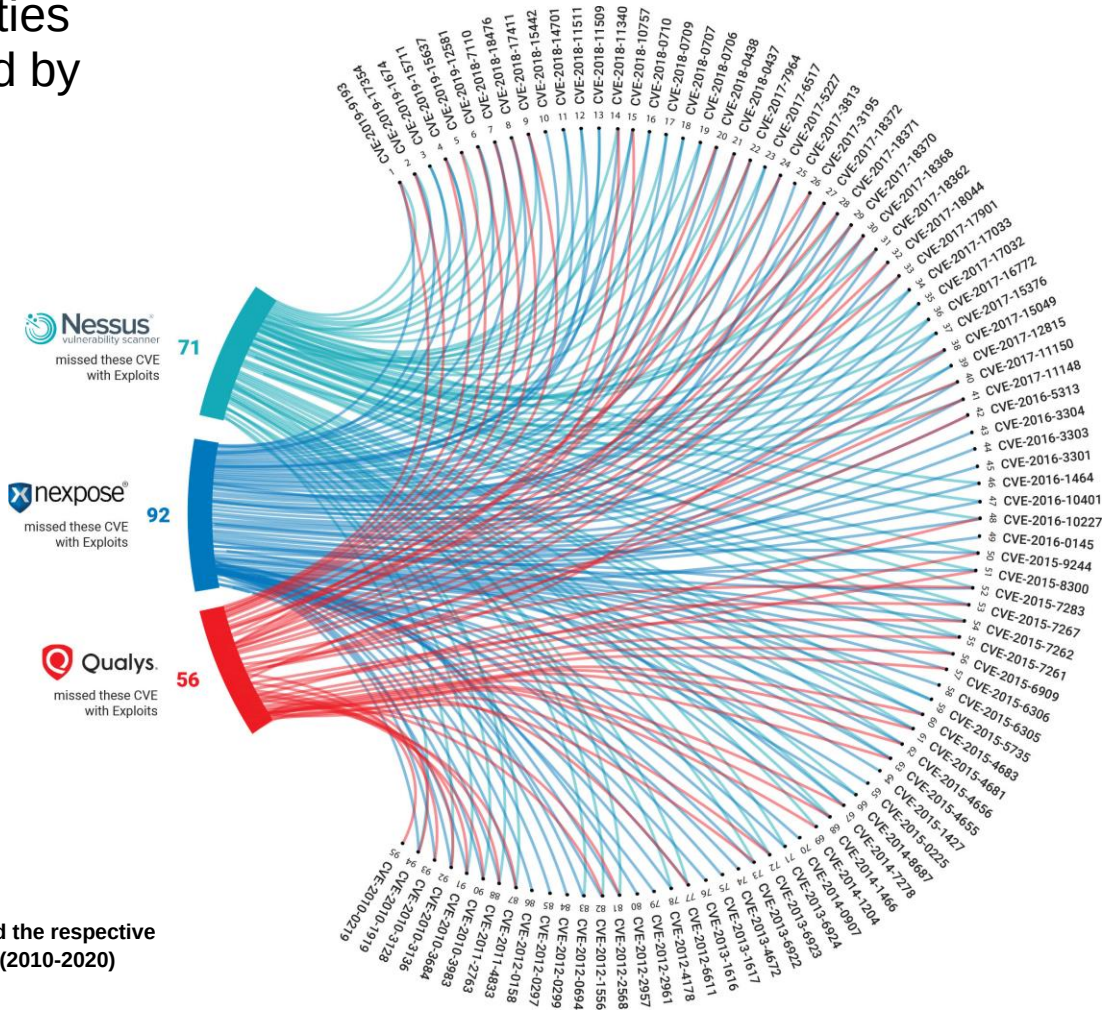

Figure 6: Scanners and the respective CVEs missed by them (2010-2020)

Here is a list of top vulnerabilities detected in each technology that needs to be fixed immediately. You can check out the Appendix II for a complete list of CVEs.

Top three Vulnerabilities

Vendor	Vulnerabilities	Why do you need to fix this immediately?
VPN		
Pulse Secure	CVE-2019-11510	This vulnerability when exploited allows an unauthenticated remote attacker to send a specially crafted URL and perform an arbitrary file reading. This was exploited in the wild to inject the 'Sodinokibi' ransomware as of January 2020.
Fortinet	CVE-2019-15711	This vulnerability has a PE exploit that may allow a user with the low privilege to run system commands under root privilege. This vulnerability is also not detected by Nessus, Nexpose, and Qualys Scanners.
Pulse Secure	CVE-2019-11539	This vulnerability allows an authenticated attacker to inject and execute commands through the admin web interface.
Remote		
ConnectWise	CVE-2017-18362	In February 2019, attackers have actively exploited this in the wild, to download and execute ransomware payloads on all endpoints managed by the VSA server. This vulnerability is missed by Nessus, Nexpose, and Qualys scanners.
BeyondTrust	CVE-2017-12815	Successful exploitation of this vulnerability results in file creation/modification/deletion in

		the operating system and with privileges of the user that ran the Java applet. This vulnerability is not detected by Nessus, Nexpose, and Qualys Scanners.
Citrix	CVE-2019-19781	This critical vulnerability allows unauthenticated remote attackers to execute commands on the targeted server after chaining an arbitrary file read/write (directory traversal) flaw. This was used during a ransomware attack in December 2019.
Enterprise Database		
MongoDB	Nil	MongoDB was subjected to a ransomware attack called "The MongoDB Apocalypse" started by the Harak1r1 group in 2017 as it is easy to find with no default credentials.
Postgresql	CVE-2019-9193	This vulnerability is not detected by Nessus, Nexpose, and Qualys scanners. This vulnerability when exploited helps to execute arbitrary code in the context of the database's operating system user. This functionality is enabled by default and can be abused to run arbitrary operating system commands on Windows, Linux, and macOS.
Mysql	CVE-2014-1466	SQL injection vulnerability in CSP MySQL User Manager 2.3 allows remote attackers to execute arbitrary SQL commands via the login field of the login page.
Web Proxy		
Cisco	CVE-2018-0438	This vulnerability is not detected by Nessus, Nexpose, and Qualys scanners and when exploited could allow an authenticated, local attacker to elevate privileges to Administrator.
Cisco	CVE-2018-0437	This vulnerability is not detected by Nessus, Nexpose, and Qualys scanners and when exploited could allow an authenticated, local attacker to elevate privileges to Administrator.
Forcepoint	CVE-2015-5718	This vulnerability allows remote administrators to cause a denial of service (crash) via a crafted diagnostic command line request.
Backup & Storage		
Vmware	CVE-2019-6110	This server vulnerability was caused due to Open SSH accepting and displaying arbitrary ‘Standard Error Output’. This can cause a malicious server or man-in-the-middle attacker to manipulate the client’s output. This was used as a part of injecting Ryuk Ransomware.
Western Digital	CVE-2018-20685	This vulnerability allows remote SSH servers to bypass intended access restrictions and modify the permissions of the target directory. This was associated with the Ryuk Ransomware.
Western Digital	CVE-2019-6109	This vulnerability allowed attackers to perform a ‘man-in-the-middle’ attack. It is also associated with the Ryuk Ransomware.
Online Conference		
Polycom	CVE-2015-4683	This vulnerability is not detected by Nessus, Nexpose, and Qualys scanners. It allows attackers to obtain sensitive information and potentially gain privileges over HTTP requests.
Zoom	CVE-2017-15049	This vulnerability is not detected by Nessus, Nexpose, and Qualys scanners and allows remote attackers to execute arbitrary code.
Lifesize	CVE-2011-2763	This vulnerability is not detected by Nessus, Nexpose, and Qualys scanners and when exploited it allows remote attackers to execute arbitrary commands.
Web Gateway		
Symantec	CVE-2016-5313	This vulnerability allows remote authenticated users to execute arbitrary OS commands.
Symantec	CVE-2013-1617	This vulnerability allows remote authenticated administrators to execute arbitrary SQL commands.
Symantec	CVE-2013-1616	This vulnerability allows remote attackers to execute arbitrary commands by injecting a command into an application script.

CRM		
SugarCRM	CVE-2011-4833	This vulnerability allows remote attackers to execute arbitrary SQL commands. It is not detected by Nessus, Nexpose, and Qualys scanners.
SAP	CVE-2018-2380	This vulnerability allows remote command execution via log injection.
SugarCRM	CVE-2012-0694	This vulnerability allows remote attackers to execute arbitrary PHP code and is not detected by Qualys scanner.
Business Intelligence		
SAP	CVE-2010-0219	This vulnerability is not detected by scanners Nessus and Nexpose and allows remote attackers to execute arbitrary code by uploading a crafted web service.
SAP	CVE-2010-3983	This vulnerability allows remote authenticated users to gain privileges that might be used to execute arbitrary code.
Tableau	CVE-2014-1204	Not detected by Nexpose scanner and has web app vulnerability associated with it. The vulnerability allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.

Conclusion

In this report, we have seen the vulnerabilities of various enterprise technologies, and the impact they can have on the security of an organization. **Not all organizations scan 100% of their internal assets**; even if they did, the probability of upgrading or patching is low for various reasons. Some of the reasons could be arduous and potentially risky as it may cause downtime or backward compatibility issue or failure of a legacy system, often led by "if it's not broken, don't fix it" mentality.

In these cases, IT administrators must have a clear insight into the real-world risk of vulnerabilities during this pandemic. These internal assets never needed connectivity from the outside (to a remote employee), so they were safe. Because of COVID-19, all employees (100%) have been asked to work-from-home. To accommodate them, IT administrators may have opened or modified permissions for allowing access to these technologies (remotely). This is the perfect opportunity for threat actors to gain access by leveraging a combination of vulnerabilities across these technologies, which were considered secure, a few weeks ago.

This makes it particularly important for CISO's and security teams to be aware that 100% scanning of assets is not an option anymore. If not done, such decisions can ultimately impact the security of the applications, databases, backups, and the organization itself. IT teams should not conflate the lack of weaponization with safety. Other technologies relatively show low weaponization, yet have relatively high numbers of vulnerabilities overall, which carry potential risk for the organization.

Ultimately organizations should have a good understanding of the overall attack surface of the various technologies, and the specific weaknesses that they contain. To achieve this, an organization must implement a continuous scanning program across 100% of their internal

About Cyber Security Works

CSW is a professional services firm focused on risk based vulnerability management and penetration testing. We offer 100% vulnerability assessment and penetration testing coverage of all digital assets, from infrastructure to code, and replicate a threat actor's lateral movement.

CSW uses several vulnerability and threat signals to help the customer's to understand cyber exposure from internal and external in a matter of hours, letting their internal teams get back to focusing on remediating vulnerabilities that matter the most and address most strategic security priorities that are unique to their business.

Since 2010, the firm has provided security consulting services to the world's leading organizations working within multiple sectors, government agencies, private organizations in Technology, Banking, Finance, Oil & Gas, Telecommunications, Information Technology Services, Healthcare, and eCommerce to help secure their products, applications, networks, and cloud with:

- Vulnerability Management as a Service
- Penetration Testing as a Service
- Red Teaming
- PCI-ASV / PCI-QSA compliance

The company has offices in Chennai, India, Albuquerque, NM, Singapore, and Dubai, UAE.

Visit our website **www.cybersecurityworks.com** for more information about our services or reach out to us at **+91 44 42089337** / **info@cybersecurityworks.com**

Appendix I

List of vendors who went under our microscope.

VPN

Cisco
Fortinet
Citrix
Palo Alto
Pulse Secure
Check Point
F5
Zscaler
Google
WatchGuard
Apple
Mobileiron
HPE Aruba)
AT&T
Systancia
Cradlepoint
OpenVPN
SonicWall

Web Proxy

Symantec
Cisco
Fortinet
F5
IBM
Akamai
HP Praesidium
SUN
Forcepoint

Remote Access Service

TeamViewer
AnyDesk
realvnc/vnc
Zoho
Apple
Citrix
TightVNC
ConnectWise
Google
Microsoft
LogMeIn
GoToMyPC
SolarWinds
BeyondTrust
LogMeIn
Parallels
Devolution
Mobatek

Web Gateway

Barracuda
Symantec
Forcepoint
Trend Micro
McAfee
Sangfor
ContentKeeper
iboss
Menlo Security
Zscaler
Check Point
Cisco

Database

MySQL
Microsoft
Postgres
Oracle
Elasticsearch
MongoDB Inc.
IBM
Amazon
IBM
SAP
IBM
Open
Redis Labs
Couchbase INC
Apache
Eponymous company
TmaxSoft
SQLite
Firebird
Teradata Corporation

CRM

Salesforce
Oracle
Pegasystem
Microsoft
SAP
Zendesk
Creatio(formerly bpm online)
ServiceNow
SugarCRM
Verint
NetSuite
Appian
Freshworks
CRMNext
Infor
eGain
Aptean
Insightly
HubSpot
Zoho

Data Storage

Acronis
Asustor
AVM
CloudBerryLab
Drobo
EMC
Intel
Linux
Meditech
Microsoft
Netapp
NTP
OpenBSD
OpenSUSE
Oracle
PalletsProjects
Paloalto Networks
Pivotal Software
PureStorage
RedHat
Seagate
Siemens
Terra-master
Veeam
Veritas
VMware
Western Digital
WinSCP
Zyxel

BI

Microsoft
Tableau
Tibco
Qlik
ThoughtSpot
MicroStrategy
Looker
Salesforce
Oracle
Sisense
SAP
Yellowfin
IBM
Domo
Infor
Information Builders
Pyramid Analytics
Logi Analytics
Board International
Alibaba

Backup

Buffalo
Commvault
Dell EMC
Fedora
Fujitsu
HP
HPE
IBM
ISC
NEC
NetBSD
Philips
QNAP
SGI
Sharp
SUN
Synology
XEN
Xiaomi
Yamaha

Online Conference

Zoom Video Communications
Microsoft
Google
Cisco
Blue jeans Network
Logmein
Adobe
Polycom corporation
Life Size
PGI
Starleaf
Teamviewer
Avaya
Intermedia.net
Trueconf
Enghouse systems
pexip
Hauwei
webex_communications
skype
skype_technologies

Appendix II

List of CVE's (2010-2020) that were missed by all three top scan solutions having exploits.

✗ - Missed

CVE ID	Nessus	Nexpose	Qualys
CVE-2019-15711	✗	✗	✗
CVE-2018-7110	✗	✗	✗
CVE-2017-18362	✗	✗	✗
CVE-2017-12815	✗	✗	✗
CVE-2018-18476	✗	✗	✗
CVE-2018-10757	✗	✗	✗
CVE-2015-9244	✗	✗	✗
CVE-2014-1466	✗	✗	✗
CVE-2018-0438	✗	✗	✗
CVE-2018-0437	✗	✗	✗
CVE-2011-4833	✗	✗	✗
CVE-2018-17411	✗	✗	✗
CVE-2010-3983	✗	✗	✗
CVE-2019-12581	✗	✗	✗
CVE-2018-11340	✗	✗	✗
CVE-2017-7964	✗	✗	✗
CVE-2017-5227	✗	✗	✗
CVE-2017-18372	✗	✗	✗
CVE-2017-18371	✗	✗	✗
CVE-2017-18370	✗	✗	✗
CVE-2017-18368	✗	✗	✗
CVE-2017-17901	✗	✗	✗
CVE-2017-11150	✗	✗	✗
CVE-2017-11148	✗	✗	✗

Appendix II (Continued)

List of CVE's (2010-2020) that were missed by three top scan solutions.

✗ - Missed

CVE ID	Nessus	Nexpose	Qualys
CVE-2016-10227	✗	✗	✗
CVE-2015-7267	✗	✗	✗
CVE-2015-7262	✗	✗	✗
CVE-2015-7261	✗	✗	✗
CVE-2015-6909	✗	✗	✗
CVE-2015-4656	✗	✗	✗
CVE-2015-4655	✗	✗	✗
CVE-2014-7278	✗	✗	✗
CVE-2013-6923	✗	✗	✗
CVE-2013-6922	✗	✗	✗
CVE-2012-2568	✗	✗	✗
CVE-2012-1556	✗	✗	✗
CVE-2010-1919	✗	✗	✗
CVE-2017-15049	✗	✗	✗
CVE-2015-8300	✗	✗	✗
CVE-2015-4683	✗	✗	✗
CVE-2015-4681	✗	✗	✗
CVE-2012-6611	✗	✗	✗
CVE-2011-2763	✗	✗	✗
CVE-2010-3136	✗	✗	✗
CVE-2010-3684	✗	✗	✗
CVE-2019-17354	✗	✗	✗
CVE-2015-7283	✗	✗	✗
CVE-2019-9193	✗	✗	✗