CSW Cyber SecurityWorks

April - 2020

COVID-19 Cyber Risk in Working Remotely

Cyber Risk in Online Conference

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.

Purpose of this Report

This is the second report in the ‘Cyber Risk in working remotely’ series. This report focuses exclusively on different online conference solutions and highlights their CVEs (Common Vulnerabilities and Exposures) from different perspectives.

In this report we bring you -

1. **Conferencing solution with the most weaponized CVEs**
2. **Call out CVEs that can be triggered remotely**
3. **Rate of weaponization over the last ten years**
4. **Prioritize vulnerabilities based on weaponization**
5. **Call out the exploitable CVEs that go undetected by the top scanners**

Introduction

The first report in the Cyber Risk in Working Remotely series gave you an overall view of the various vulnerabilities that exist in tech stacks and applications. In this report, we will examine online conference solutions that are being used and learn how safe they are…

Corona Virus (COVID) Pandemic has forced people all around the world to work remotely. Official meetings, conferences, training sessions, seminars, classes, etc. are being conducted through online conferencing solutions.

One can't get around the fact that employees need to collaborate through online conference solutions to discuss sensitive internal company affairs. High-level meetings that were once held within the four walls of office space are now being discussed over video calls.

Sadly, most companies do not have a policy in place for the employees to follow during an online conference, especially while discussing/sharing screens that contain sensitive and confidential information about their organization, products, and services.

With the pandemic induced lockdown extending in most places, online conferencing solutions present a perfect opportunity for threat actors to breach and steal data from organizations.

Ideally, your scan system should be alerting you about vulnerabilities that exist in these applications, but how far they are able to that, you will learn from this report.

Vulnerable online conferencing solutions

Online Conferencing is one of the key mediums through which users maintain communication to share and review their work while working remotely. While these solutions have the best speech recognition and recording capabilities, they also have many security vulnerabilities as well.

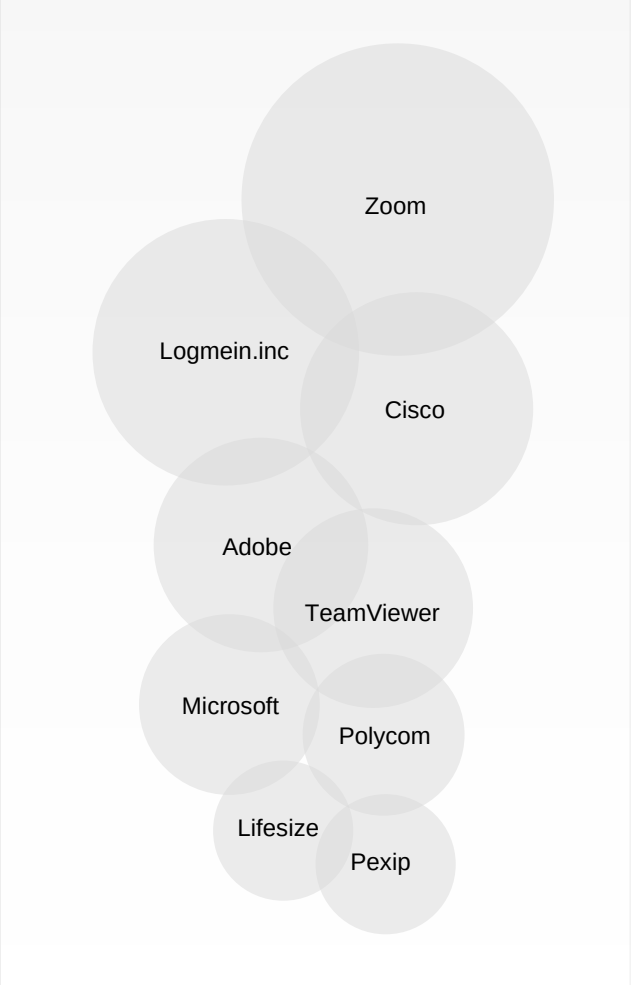

Figure 1: Online Conferencing vendors

For our analysis, we have selected some of the leading vendors from Gartner and Forrester's research and put them under our microscope. The list of all vendors considered for this study can be viewed in Appendix I.

Overview of Vulnerabilities

Online Conferencing has been around for over two decades. Since the beginning of 2020, the usage of online conference solutions has grown by 57%-84%*. This increase in usage when juxtaposed with the vulnerability data given below, is a cause for concern.

Figure 1 shows the list of vendors in the online conferencing space. Some of these vendors have both critical and high vulnerabilities (CVEs). We analyzed a total of **877** vulnerabilities across all vendors from the year 2010 through February 2020. Our research shows that **4.4%** of these vulnerabilities are weaponized and can be executed remotely.

Vulnerabilities by Vendors

We plotted the count of vulnerabilities of all vendors and discovered some interesting trends. Figure 2 shows the distribution of vulnerabilities based on Common Vulnerability Scoring System Version 2 (CVSS 2). Cisco and Huawei combined have the highest number of critical, high & medium vulnerabilities, which constitutes **78%** of the total vulnerabilities.

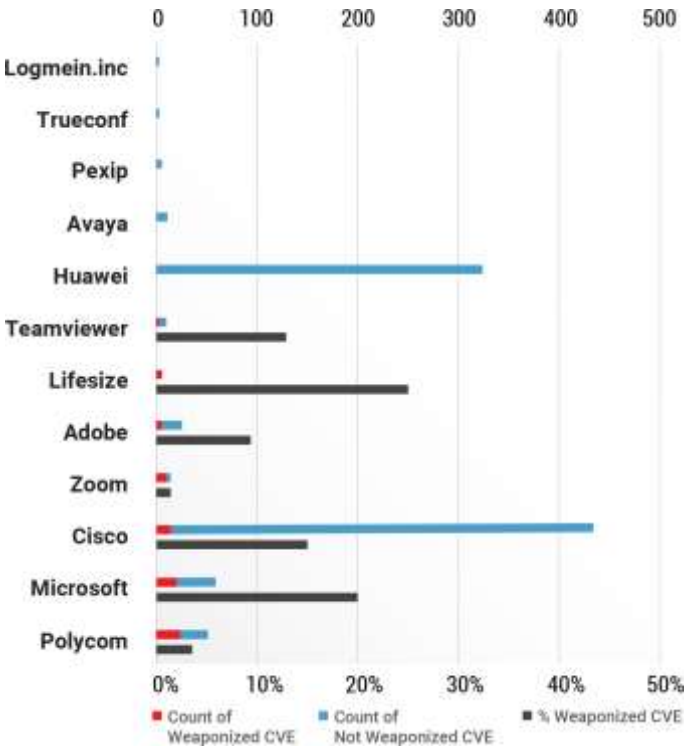

Figure 2: Weaponization of CVEs for Online Conferencing technologies (2010-2020)

But while considering the severity of issues, Cisco and Microsoft have the highest number of critical vulnerabilities, constituting **94%** of the total critical CVEs as seen in Figure 3. Microsoft also leads along with Polycom on the number of weaponized vulnerabilities. Together contributing to **58%** of weaponization (**22** out of **38** CVEs are weaponized).

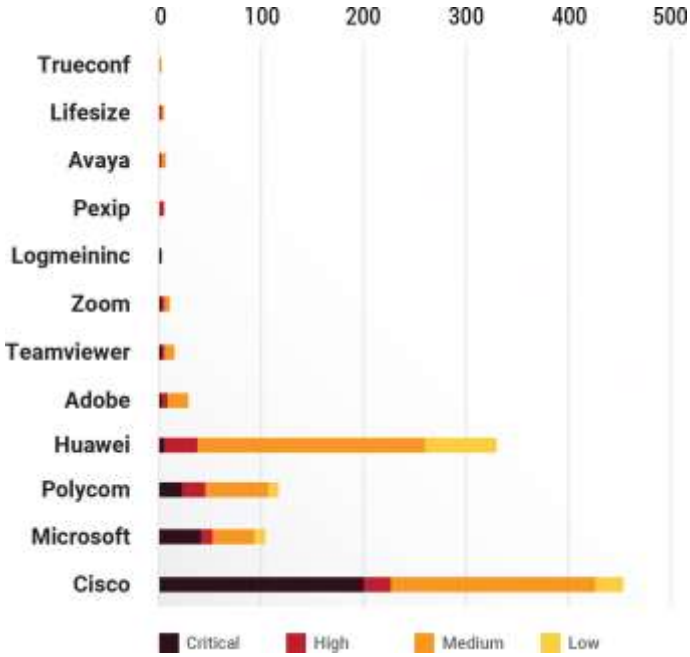

Figure 3: CVE Distribution for Online Conferencing Technologies (2010-2020)

Vulnerabilities – Over the years

We next analyzed the dataset by the year to see how the weaponization of vulnerabilities has been changing year after year. Figure 4 shows each year broken by vulnerabilities

* https://productiv.com/productiv-insights-video-collaboration-in-the-age-of-covid-19/

Overview of Vulnerabilities (Continued)

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 were high in 2015 and 2016. Whereas, the count of vulnerabilities discovered spiked in 2017 and continued to be very high in 2018 and 2019 when compared to 2015 and 2016. It can be assumed that these are waiting to get weaponized**.**

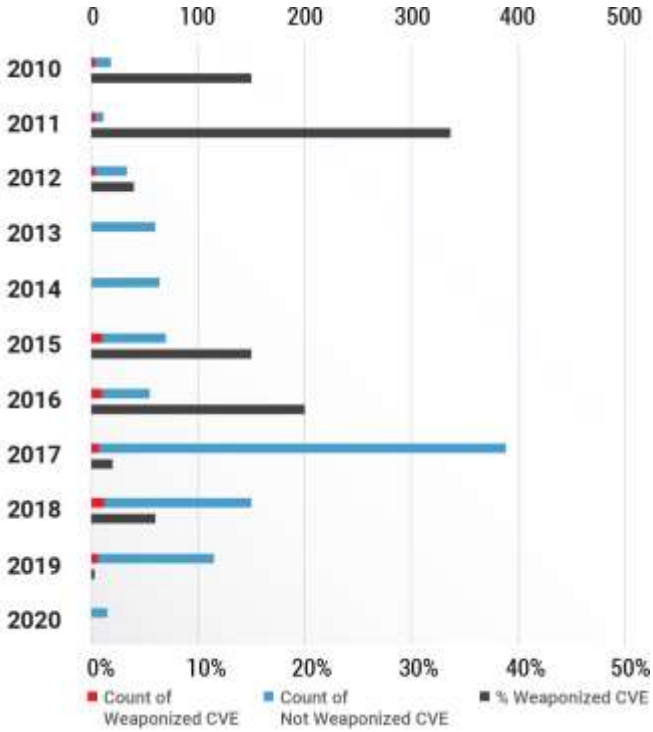

Figure 4: Weaponization of CVEs (2010 -2020)

Vulnerability Prioritization by Weaponization

On further analysis of the vulnerabilities with high impact, we extracted those that enabled remote code execution (RCE), and privilege escalation (PE). Figure 5 shows a pyramid that could be useful for security teams to prioritize their remediation.

We found 17 vulnerabilities either enabled Remote Code Execution (RCE) or Privilege Escalation (PE) out
of the **877** vulnerabilities. All RCE and PE capable vulnerabilities are weaponized.

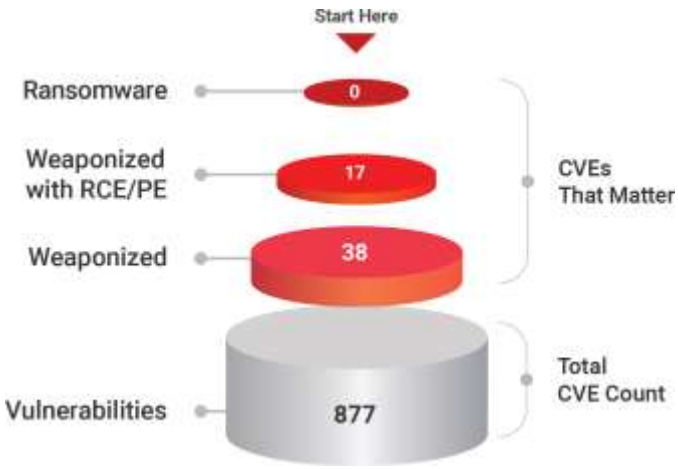

Figure 5: Vulnerability Prioritization across Online Conferencing Technologies (2010-2020)

Vulnerabilities Missed by Top Scanners

We analyzed the data further by comparing the CVEs with the plugins from some of the best scanners. Surprisingly, leading scanners in the market have failed to detect critical and high vulnerabilities that have weaponized exploits in the wild. Table 1 below shows the count of vulnerabilities from 2010 to 2020 that were missed by scanners.

The Chord diagram (Figure 6) shows the pictorial representation of the same. To view the list of undetected CVEs, please refer Appendix II.

	NESSUS	NEXPOSE	QUALYS
CISCO	2	3	0
LIFESIZE	1	1	1
MICROSOFT	2	6	1
TEAMVIEWER	0	1	1
POLYCOM	4	4	4
ZOOM	1	1	1
TOTAL	**10**	**16**	**8**

Table 1: Count of Vulnerabilities Missed by top Scanners (2010-2020)

Vulnerabilities Undetected by Top Scanners

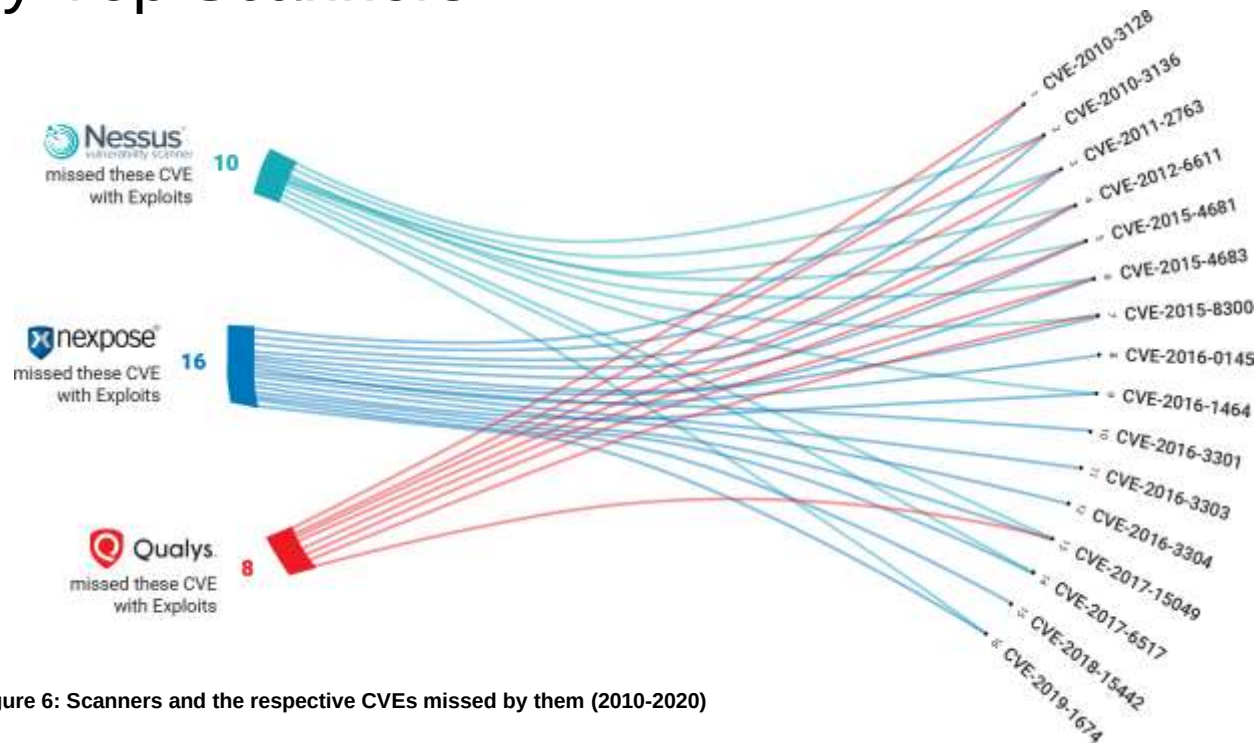

Figure 6: Scanners and the respective CVEs missed by them (2010-2020)

Conclusion

While the vulnerabilities detected in Zoom continue to draw media scrutiny and they are, by no means, the only video conferencing solution that can be penetrated. Based on our research, we looked at the attack surface of twenty online conference solutions. We identified **877** vulnerabilities across all of them. **4.4%** of these are weaponized with RCE/PE. (Remote Code Execution / Privilege Escalation).

- Years 2015 and 2016 had **44** and **34** counts of vulnerabilities respectively, between the two the highest rate of weaponization was in 2016.
- The count of vulnerabilities was highest in 2017
- Cisco and Huawei together contribute to **78%** of critical, high, and medium vulnerabilities
- Cisco and Microsoft together contribute to **94%** of critical vulnerabilities
- Microsoft and Polycom together contribute to **58%** of weaponized vulnerabilities
- **CVE-2015-8300**, **CVE-2015-4683**, **CVE-2015-4681**, and **CVE-2012-6611** in Polycom are not detected by the three top scanners
- **CVE-2017-15049** in Zoom is not detected by the three top scanners
- **CVE-2011-2763** and **CVE-2010-3136** in Lifesize and Microsoft respectively are not detected by the top three scanners
- The above-listed CVEs are all weaponized and are RCE/PE enabled.

IT teams shouldn't conflate the lack of weaponization with safety. The alarming count of vulnerabilities in 2017, 2018, and 2019 is a disturbing trend.

We believe that these are waiting to get weaponized and therefore recommend a continuous scanning program across 100% of organization assets.

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.

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 three top scanners.

✓ - Detected ✗ - Missed

No.	CVE ID	Vendor	Nessus	Nexpose	Qualys
1	CVE-2015-8300	Polycom	✗	✗	✗
2	CVE-2015-4683	Polycom	✗	✗	✗
3	CVE-2015-4681	Polycom	✗	✗	✗
4	CVE-2012-6611	Polycom	✗	✗	✗
5	CVE-2017-15049	Zoom	✗	✗	✗
6	CVE-2011-2763	Lifesize	✗	✗	✗
7	CVE-2010-3136	Microsoft	✗	✗	✗
8	CVE-2018-15442	Cisco	✓	✗	✓
9	CVE-2019-1674	Cisco	✗	✗	✓
10	CVE-2016-1464	Cisco	✗	✗	✓
11	CVE-2017-6517	Microsoft	✗	✗	✓
12	CVE-2010-3128	TeamViewer	✓	✗	✗
13	CVE-2016-0145	Microsoft	✓	✗	✓
14	CVE-2010-3301	Microsoft	✓	✗	✓
15	CVE-2010-3303	Microsoft	✓	✗	✓
16	CVE-2010-3304	Microsoft	✓	✗	✓