CSW Cyber SecurityWorks

June - 2020

COVID-19 Cyber Risk in Working Remotely

Cyber Risk in CRM

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 eighth report in the ‘Cyber Risk in working remotely’ series. In this report, we compare various Customer Relationship Management (CRM) solutions and highlight their CVEs (Common Vulnerabilities and Exposures) from different perspectives.

1. Customer relationship management (CRM) solution that has more weaponized CVEs
2. Call out CVEs that can be triggered remotely
3. Rate of weaponization over the last ten years
4. Prioritizing vulnerabilities based on weaponization
5. Call out exploitable CVE that go undetected by top scanners

Introduction

This is the eighth report in the Cyber Risk in working remotely series. In this report, we will examine the various vulnerabilities that exist in popular CRM solutions.

Corona pandemic has created a challenging circumstance for employees' world over to work remotely. This has also forced their dependency on various technologies to get the work done.

Many companies have exposed their internal systems and infrastructure to remote access, which leaves them vulnerable for data loss and theft.

The CRM tools and applications that you have used so far only from the secure environment of your office space is now available on personal laptops and home PCs.

How safe are you CRM tools from a data breach? Let's find out.

Vulnerable Customer relationship management (CRM) solutions

Customer relationship management (CRM) improves business relationships and manages all your company's relationships and interactions with clients and potential customers. Attacking a CRM gives direct access to customers, internal processes, and other key factors of the company.

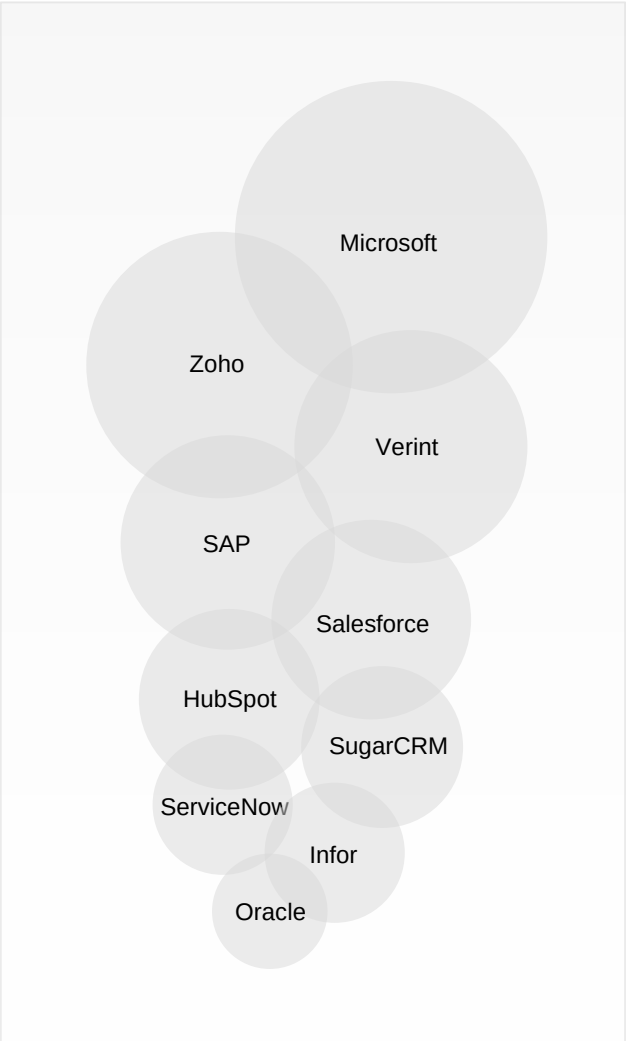

Figure 1: CRM Vendors Covered

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

CRM system is a tool that helps with contact management, sales management, productivity, and more. A CRM solution is a very powerful tool and when its vulnerabilities are exposed it provides access to threat actors to steal personal information about your employees, customers, and vendors.

Figure 1 shows the list of vendors in the customer relationship management (CRM) products. Some of these products have both critical and high vulnerabilities (CVEs). We analyzed a total of **106** vulnerabilities across all vendors from the year 2010 to 2020. Our research shows that almost **17.9%** of these vulnerabilities are weaponized and **15.7%** of these weaponized vulnerabilities can be executed remotely.

Vulnerabilities by Vendors

On graphically representing the accumulated and organized data, we come across interesting facts. **Figure 2** shows the number of weaponized and non-weaponized. Out of **19** weaponized vulnerabilities, **SugarCRM** covers **47.36%** of total weaponized vulnerabilities among other listed vendors.

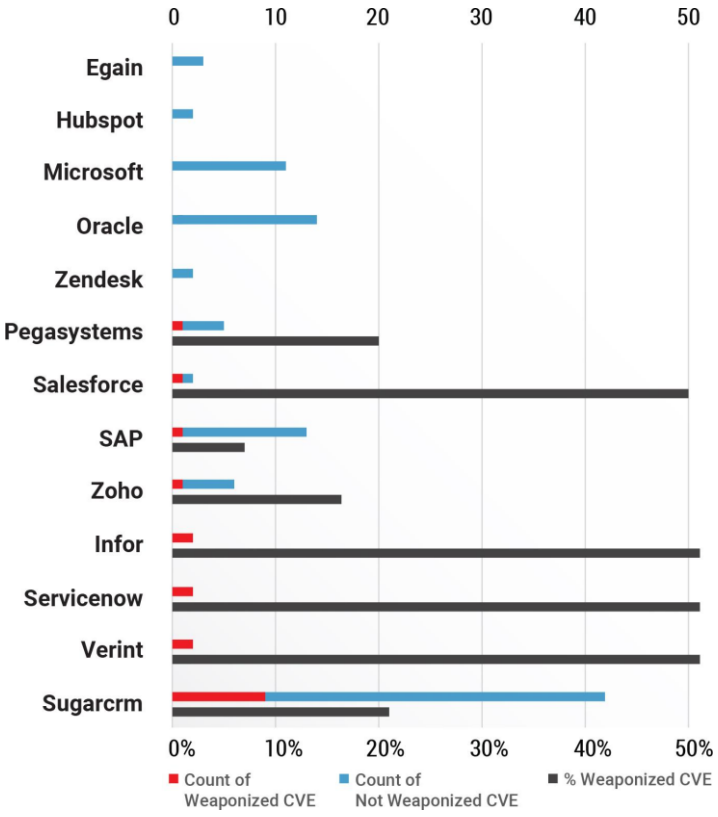

Figure 2: Weaponization of CVEs for CRM technologies (2010 -2020)

Figure 3 covers the critical, high, and other flaws that have become an entry trigger for an attacker.

Out of **5** critical vulnerabilities, **SAP** occupies **60%** of critical vulnerabilities and stands apart from other listed vendors.

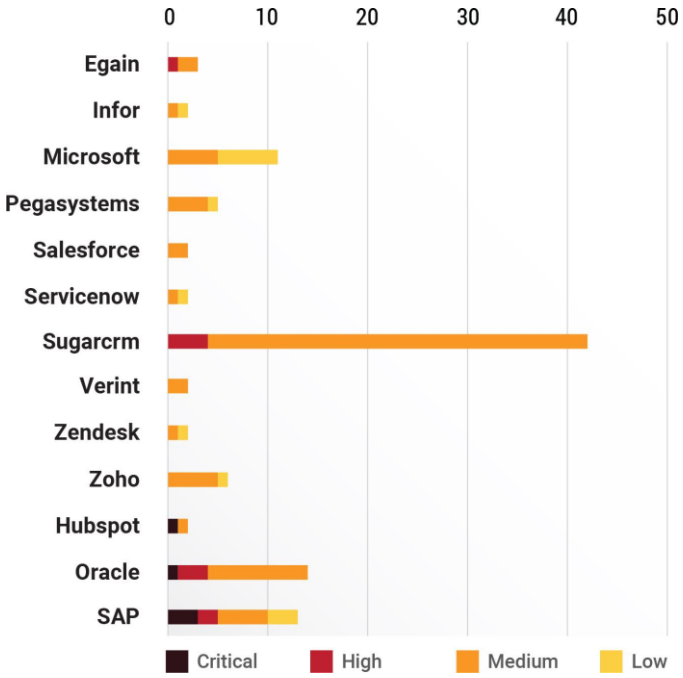

Figure 3: CVE Distribution for CRM technologies (2010 -2020)

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 that were weaponized versus those that were not. Data in 2020 only includes vulnerabilities until the end of February.

Overview of Vulnerabilities (Continued)

Here we can see a gradual rise and fall in the vulnerability count from 2017. Also, 2018 and 2019 had a surge in weaponized vulnerabilities when compared with other years.

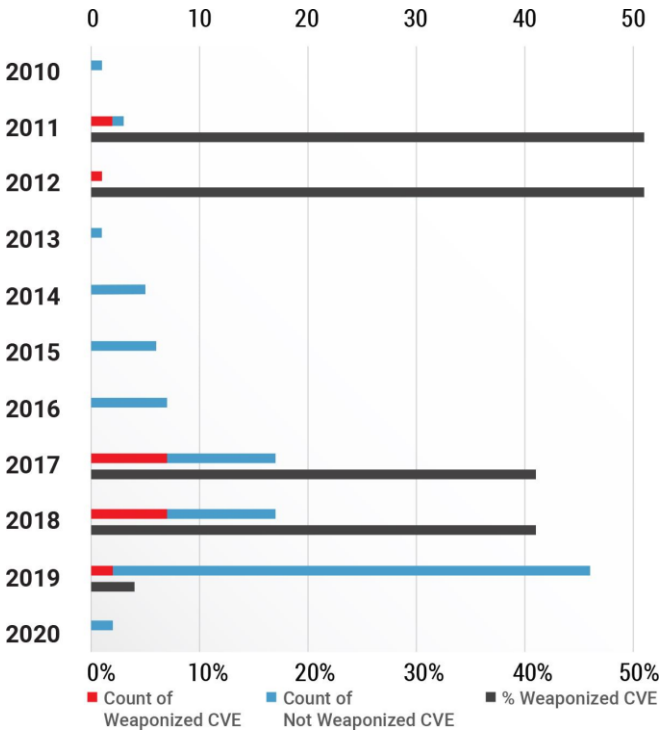

Figure 4: Weaponization of CVEs (2010 -2020)

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 **3 vulnerabilities** with either enabled remote code execution or privilege escalation out of **106 vulnerabilities.** These flaws can allow remote attackers to execute arbitrary PHP code SQL

commands.

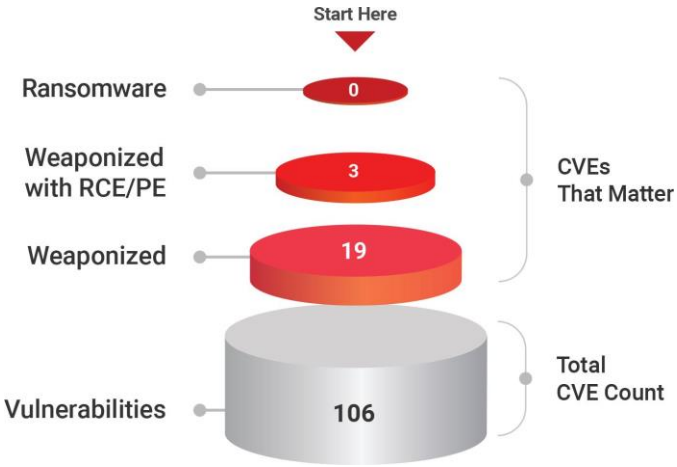

Figure 5: Vulnerabilities Prioritization Across CRM technologies (2010 -2020)

Vulnerabilities Missed by Top Scanners

We analyzed the data further by comparing the CVEs with the plugins from some of the best scanners. Surprisingly, the leading scanners fail 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 to Appendix II.

	NESSUS	NEXPOSE	QUALYS
SUGARCRM	2	2	1
Total	**2**	**2**	**1**

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

Vulnerabilities Undetected by Top Scanners

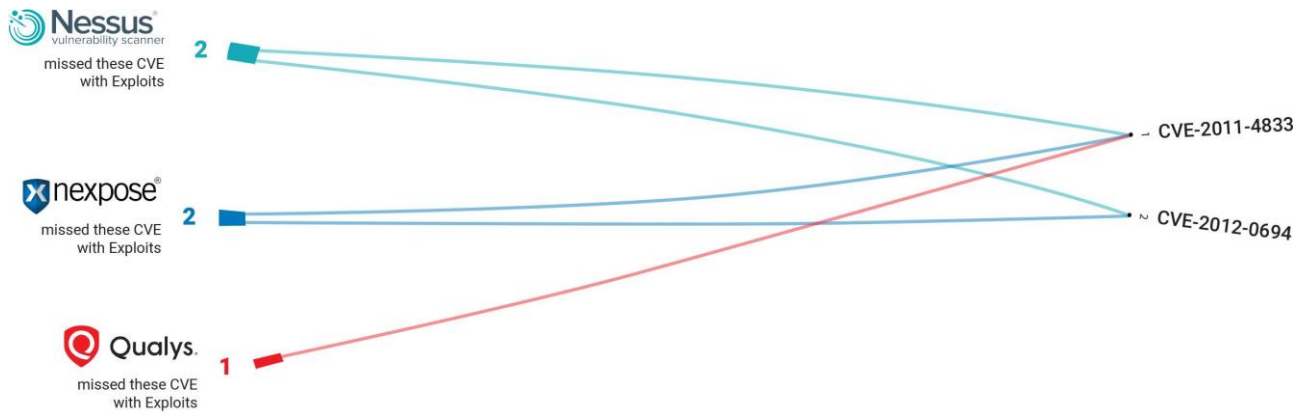

Figure 6: Scanners and the respective CVEs missed by them (2010-

Conclusion

Based on our research, we looked at the attack surface of 13 customer relationship management (CRM) solutions. We identified **106** vulnerabilities across all the identified products. **17.9%** of these are weaponized with **15.7%** of them having RCE/PE. (Remote Code Execution / Privilege Escalation).

- In the years 2017 and 2018 had 17 each respectively whereas in the year 2019 the count of vulnerabilities rose to **46**.
- The count of vulnerabilities was highest in 2019.
- SAP contributes to **60%** of the critical, high, and medium vulnerabilities among all 13 products.
- SugarCRM contributes to **47.3%** of the weaponized vulnerabilities.
- **CVE-2011-4833** and **CVE-2012-0694** were not detected by three top scanners.

The lack of weaponization doesn't undermine the risk involved. The alarming count of vulnerabilities in 2017, 2018, and 2019 is disturbing because these are just waiting to get weaponized. We recommend a continuous scanning program across 100% of your assets.

About Cyber Security Works

CSW is the only Cybersecurity Start-up with the highest number of Zero-Day disclosures. Our prime focus is to discover and prioritize vulnerabilities that matter. We continuously monitor vulnerability data from 100+ sources to understand cyber exposure from inside and outside. We are also the only company that offers 100% coverage of all digital assets, from infrastructure to code and replicate a threat actor's movements.

Vulnerability Management as a Service, Penetration Testing as a Service, Red Teaming, and PCI-ASV / PCI-QSA compliance are some of the services that we provide our customers. We have extensively worked with government agencies, private organizations in Technology, Banking, Finance, Oil & Gas, Telcos, ITES, Healthcare, and eCommerce.

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.

Customer Relationship Management (CRM)

- eGain
- HubSpot
- Infor
- Microsoft
- Pegasystems
- Salesforce
- SAP
- ServiceNow
- SugarCRM
- Verint
- Zendesk
- Zoho

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-2011-4833	SugarCRM	✗	✗	✗
2	CVE-2012-0694	SugarCRM	✗	✗	✓