

[Return to the VPLS Blog](#)

## Blog Post

# Top Exploited Cybersecurity Vulnerabilities of 2020 and 2021 (So Far)

Published

Oct 19, 2021

Written by

**John Headley**

Filed under

[Cybersecurity](#), [Managed Security](#), [Managed Services](#)

The top cybersecurity vulnerabilities of 2020 and 2021, which are being routinely exploited by malicious actors, have been compiled into a list via a joint effort by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S. Federal Bureau of Investigation (FBI).

A majority of the most targeted vulnerabilities in both 2020 and 2021 affect remote work, VPNs, or cloud-based technologies. This includes giants such as Microsoft (Windows, Exchange, SharePoint), Fortinet (FortiGate), and VMware (vCenter Server).

Note as you review the list below that many of the top exploited vulnerabilities

were vulnerabilities discovered years before. This is a red flag that a lot of organizations do not have a vulnerability management process, which is something we will discuss later in the post.

## The List

### Top Routinely Exploited CVEs in 2020

<b>Vendor</b>	<b>Product</b>	<b>CVE</b>	<b>Severity</b>	<b>CVSSv3 Score</b>
Atlassian	Crowd and Crowd Data Center	CVE-2019-11580	Critical	9.8
Citrix	Application Delivery Controller (ADC) and Gateway	CVE-2019-19781	Critical	9.8
Drupal	Drupal	CVE-2018-7600	Critical	9.8
F5	BIG-IP	CVE-2020-5902	Critical	9.8
Fortinet	FortiGate	CVE-2018-13379	Critical	9.8
Microsoft	Microsoft Office	CVE-2017-11882	High	7.8
Microsoft	SharePoint	CVE-2019-0604	Critical	9.8
Microsoft	Windows	CVE-2020-0787	High	7.8

Microsoft	Windows Server	CVE-2020-1472	Critical	10
MobileIron	Core & Connector	CVE-2020-15505	Critical	9.8
Pulse Secure	Pulse Connect Secure (PCS)	CVE-2019-11510	Critical	10
Telerik	Progress Telerik UI for ASP.NET AJAX	CVE-2019-18935	Critical	9.8

## Top Routinely Exploited CVEs in 2021

Last Updated on August 20, 2021

<b>Vendor</b>	<b>Product</b>	<b>CVE</b>	<b>Severity</b>	<b>CVSSv3 Score</b>
Accellion	FTA	CVE-2021-27101	Critical	9.8
Accellion	FTA	CVE-2021-27102	High	7.8
Accellion	FTA	CVE-2021-27103	Critical	9.8
Accellion	FTA	CVE-2021-27104	Critical	9.8
Fortinet	FortiGate	CVE-2018-13379	Critical	9.8
Fortinet	FortiGate	CVE-2020-12812	Critical	9.8

Fortinet	FortiGate	CVE-2019-5591	Medium	6.5
Microsoft	Exchange	CVE-2021-26855	Critical	9.8
Microsoft	Exchange	CVE-2021-26857	High	7.8
Microsoft	Exchange	CVE-2021-26858	High	7.8
Microsoft	Exchange	CVE-2021-27065	High	7.8
Pulse Secure	Pulse Connect Secure (PCS)	CVE-2021-22893	Critical	10
Pulse Secure	Pulse Connect Secure (PCS)	CVE-2021-22894	High	8.8
Pulse Secure	Pulse Connect Secure (PCS)	CVE-2021-22899	High	8.8
Pulse Secure	Pulse Connect Secure (PCS)	CVE-2021-22900	High	7.2
VMware	vCenter Server	CVE-2021-21985	Critical	9.8

## VPLS's Advice & Recommended Next Steps

As an urgent, one-time exercise, VPLS recommends reviewing the two lists above and determining if your organization is running affected products/software. If you are, the next steps would be to patch the software to a version that is not vulnerable to the listed CVEs. In addition to patching, other mitigation steps may be necessary to protect against the vulnerability being exploited, such as a configuration change, and those will be documented in the vendor's related security advisory.

Going forward, organizations should implement a continuous vulnerability management practice if one is not already in place. A [mature cybersecurity program](#) includes vulnerability management, which is the ongoing practice of

identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities.

For organizations that require guidance on vulnerability management, or simply don't have the time to dedicate to this critical task, VPLS can perform vulnerability management for your IT department with convenient monthly or one-time services. For example, many of our customers leverage the vulnerability management practices included with our [SOC as a Service](#), which includes scanning (identifying, classifying, and prioritizing) for vulnerabilities across all assets that belong to the organization.

Extending VPLS's SOC-as-a-Service with our [Managed Firewall](#) and [Managed Network](#) services, or [Managed Servers](#) and [Managed Desktops](#) services, will ensure that VPLS is proactively remediating and mitigating the vulnerabilities related to these products for your organization so you are always one step ahead of threat actors and their malicious intentions.

### ***Need Some Help?***

---

Need some help reviewing your current security infrastructure or just want to see if there are [better options out there](#)? VPLS has the right solution for you! VPLS consistently ranks as a top Service Provider and Managed Service Provider among competitors. From Help Desk to managed SOC and security services, VPLS has an array of managed services catered to organizations big and small. [Contact VPLS for a free custom quote today.](#)

## Read More from this Author

### John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

[More from this Author](#)



**PREVIOUS**

[Network Optimization: 6 Indications Your Network...How to Optimize Your Enterprise With a Managed...](#)

**NEXT**



If you enjoyed this article, you'll probably like:



VPLS Recognized on CRN's 2022 MSP 500 List for Seventh Consecutive Year

February 15, 2022

[Read More »](#)



## 4 Must-Have Features of Top Cyber Threat Intelligence Solutions in 2021

Not all threat intelligence solutions are created equal. Here's what you need to look for when choosing a cybersecurity solution.

[START READING](#)

### Cyber Threat Intelligence Solutions in 2021: Four Must-Have Features

November 15, 2021

[Read More »](#)



## What are Managed SOC Best Practices?

SOCs were created with the goal of monitoring and improving an organization's security posture. Discover best practices for managing a SOC in this short blog post.



### How to Reach Us

November 2, 2021

#### Corporate Headquarters

600 West 7th Street, Suite 510  
Los Angeles, CA 90017

**24/7/365 Customer Service**



+1 (888) 365-2656  
support@vpls.com

### **Sales Inquiries**

+1 (888) 365-2656  
sales@vpls.com

## **WHAT WE DO**

Cloud  
Hosting  
Colocation  
Network Services  
Managed Services  
Professional Services  
VAR

## **WHO WE SERVE**

Financial Services  
Healthcare and Life Sciences  
Media & Entertainment  
Telecom  
Startup  
Enterprise  
Public Sector