CISA reveals the **top 30** most exploited **vulnerabilities** since 2020

Buckle up, folks! The feds have dropped the top 30 vulnerabilities actively used by hackers since 2020. A recent joint advisory issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA)—in conjunction with the Australian Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S. Federal Bureau of Investigation (FBI)—details the vulnerabilities that have been routinely exploited in 2020 and 2021.

What are you waiting for? Start sweeping your network for the CVEs mentioned below and ensure you're patched to save yourself from joining the densely populated club of cyber casualties.

Notorious vulnerabilities routinely exploited in 2020

AFFECTED PRODUCTS	CVE	CVSS	IMPACT
Citrix Application Delivery Controller (ADC) and Citrix Gateway	CVE-2019-19781	9.8	Directory traversal
Pulse Connect Secure	CVE-2019-11510	10	Arbitrary file reading
Fortinet FortiOS	CVE-2018-13379	9.8	Path traversal vulnerability leading to system file leak
F5 BIG-IP	CVE-2020-5902	9.8	Remote code execution
MobileIron Core & Connector	CVE-2020-15505	9.8	Remote code execution
Microsoft Exchange Server	CVE-2020-0688	8.8	Memory corruption
Atlassian Confluence Server	CVE-2019-3396	9.8	Remote code execution
Microsoft Office	CVE-2020-15505	7.8	Memory corruption
Atlassian Crowd and Crowd Data Center	CVE-2019-11580	9.8	Remote code execution
Drupal	CVE-2018-7600	9.8	Remote code execution
Telerik UI for ASP.NET AJAX	CVE-2019-18935	9.8	Remote code execution
Microsoft SharePoint	CVE-2019-0604	9.8	Remote code execution
Windows Background Intelligent	CVE-2020-0787	7.8	Elevation of privilege
Windows Netlogon	CVE-2020-1472	10	Elevation of privilege

What caught hackers' attention in 2021?

AFFECTED PRODUCTS	CVE	CVSS	IMPACT
Pulse Secure Pulse Connect Secure	CVE-2021-22893	10	Remote arbitrary code execution
	CVE-2021-22894	8.8	Remote arbitrary code execution
	CVE-2021-22899	8.8	Remote code execution
	CVE-2021-22900	7.2	Code injection
Exchange Microsoft Exchange Server	CVE-2021-26855	9.8	Remote code execution
	CVE-2021-26857	7.8	Remote code execution
	CVE-2021-26858	7.8	Remote code execution
	CVE-2021-27065	7.8	Remote code execution
Accellion Accellion	CVE-2021-27101	9.8	SQL injection
	CVE-2021-27102	7.2	OS command injection
	CVE-2021-27103	9.8	Server-side request forgery (SSRF)
	CVE-2021-27104	9.8	OS command execution
vmware VMware	CVE-2021-21985	9.8	Remote code execution
FORTINET Fortinet	CVE-2018-13379	9.8	Path traversal
	CVE-2020-12812	9.8	Improper authentication
	CVE-2019-5591	6.5	Configuration vulnerability

What can we learn from these exploits?

Surprisingly, dated vulnerabilities are still ripe for exploitation, as evidenced by the ongoing exploitation of CVE-2017-11882, which is several years old. It's also an indicator of how common it is for many organizations to continue using affected products unpatched.

Zero-day attacks are rare. Attackers are more likely to exploit known vulnerabilities of prominent products, because it allows them to weaponize flaws against broad target sets worldwide.

The unprecedented expansion into remote work accounts for the increased exploitation of vulnerabilities in 2020 and 2021. The rapid paradigm shift made it difficult for security teams to keep pace with routine patching on remote machines.

Four of the most targeted vulnerabilities exist in VPN gateways and other tools that offer remote access.

How to keep vulnerabilities at bay

The CISA urges organizations to implement a centralized patch management system and prioritize patches to the most exploited vulnerabilities. If you're looking for the right tool, look no further. ManageEngine brings you three offerings that can indeed make patching a breeze for you. From continually sweeping your distributed endpoints for security flaws to testing and deploying patches to them, everything can be automated from a single pane of glass.

Desktop Central

Desktop Central is a unified endpoint management and security solution that caters to the entire endpoint management life cycle, including automating patching; deploying software; taking control of remote desktops; and managing and monitoring assets, software licenses, software usage, and USB device usage; and much more.

FREE TRIAL

Vulnerability Manager Plus

Vulnerability Manager Plus is a prioritization-focused threat and vulnerability management tool for enterprises offering built-in patch management.

FREE TRIAL

Patch Manager Plus

Patch Manager Plus is an all-around patching solution offering automated patch deployment for Windows, macOS, and Linux endpoints along with over 500 third-party applications.

FREE TRIAL