2021 Top Routinely Exploited Vulnerabilities

Key Findings

Globally, in 2021, malicious cyber actors targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed vulnerabilities. For most of the top exploited vulnerabilities, researchers or other actors released proof of concept (POC) code within two weeks of the vulnerability's disclosure, likely facilitating exploitation by a broader range of malicious actors.

To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities—some of which were also routinely exploited in 2020 or earlier. The exploitation of older vulnerabilities demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor.

Top 15 Routinely Exploited Vulnerabilities

Table 1 shows the top 15 vulnerabilities U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities observed malicious actors routinely exploiting in 2021, which include:

- **CVE-2021-44228.** This vulnerability, known as Log4Shell, affects Apache's Log4j library, an open-source logging framework. An actor can exploit this vulnerability by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows a cyber actor to take full control over the system. The actor can then steal information, launch ransomware, or conduct other malicious activity.[1] Log4j is incorporated into thousands of products worldwide. This vulnerability was disclosed in December 2021; the rapid widespread exploitation of this vulnerability demonstrates the ability of malicious actors to quickly weaponize known vulnerabilities and target organizations before they patch.

- **CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065.** These vulnerabilities, known as ProxyLogon, affect Microsoft Exchange email servers. Successful exploitation of these vulnerabilities in combination (i.e., "vulnerability chaining") allows an unauthenticated cyber actor to execute arbitrary code on vulnerable Exchange Servers, which, in turn, enables the actor to gain persistent access to files and mailboxes on the servers, as well as to credentials stored on the servers. Successful exploitation may additionally enable the cyber actor to compromise trust and identity in a vulnerable network.
- **CVE-2021-34523, CVE-2021-34473, CVE-2021-31207.** These vulnerabilities, known as ProxyShell, also affect Microsoft Exchange email servers. Successful exploitation of these vulnerabilities in combination enables a remote actor to execute arbitrary code. These vulnerabilities reside within the Microsoft Client Access Service (CAS), which typically runs on port 443 in Microsoft Internet Information Services (IIS) (e.g., Microsoft's web server). CAS is commonly exposed to the internet to enable users to access their email via mobile devices and web browsers.
- **CVE-2021-26084.** This vulnerability, affecting Atlassian Confluence Server and Data Center, could enable an unauthenticated actor to execute arbitrary code on vulnerable systems. This vulnerability quickly became one of the most routinely exploited vulnerabilities after a POC was released within a week of its disclosure. Attempted mass exploitation of this vulnerability was observed in September 2021.

Three of the top 15 routinely exploited vulnerabilities were also routinely exploited in 2020: CVE-2020-1472, CVE-2018-13379, and CVE-2019-11510. Their continued exploitation indicates that many organizations fail to patch software in a timely manner and remain vulnerable to malicious cyber actors.

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2021

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

Additional Routinely Exploited Vulnerabilities

In addition to the 15 vulnerabilities listed in table 1, U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities identified vulnerabilities, listed in table 2, that were also routinely exploited by malicious cyber actors in 2021.

These vulnerabilities include multiple vulnerabilities affecting internet-facing systems, including Accellion File Transfer Appliance (FTA), Windows Print Spooler, and Pulse Secure Pulse Connect Secure. Three of these vulnerabilities were also routinely exploited in 2020: CVE-2019-19781, CVE-2019-18935, and CVE-2017-11882.

Table 2: Additional Routinely Exploited Vulnerabilities in 2021

CVE	Vendor and Product	Type
CVE-2021-42237	Sitecore XP	RCE
CVE-2021-35464	ForgeRock OpenAM server	RCE

CVE	Vendor and Product	Type
CVE-2021-27104	Accellion FTA	OS command execution
CVE-2021-27103	Accellion FTA	Server-side request forgery
CVE-2021-27102	Accellion FTA	OS command execution
CVE-2021-27101	Accellion FTA	SQL injection
CVE-2021-21985	VMware vCenter Server	RCE
CVE-2021-20038	SonicWall Secure Mobile Access (SMA)	RCE
CVE-2021-40444	Microsoft MSHTML	RCE
CVE-2021-34527	Microsoft Windows Print Spooler	RCE
CVE-2021-3156	Sudo	Privilege escalation
CVE-2021-27852	Checkbox Survey	Remote arbitrary code execution
CVE-2021-22893	Pulse Secure Pulse Connect Secure	Remote arbitrary code execution
CVE-2021-20016	SonicWall SSLVPN SMA100	Improper SQL command neutralization, allowing for credential access
CVE-2021-1675	Windows Print Spooler	RCE
CVE-2020-2509	QNAP QTS and QuTS hero	Remote arbitrary code execution
CVE-2019-19781	Citrix Application Delivery Controller (ADC) and Gateway	Arbitrary code execution
CVE-2019-18935	Progress Telerik UI for ASP.NET AJAX	Code execution
CVE-2018-0171	Cisco IOS Software and IOS XE Software	Remote arbitrary code execution
CVE-2017-11882	Microsoft Office	RCE
CVE-2017-0199	Microsoft Office	RCE

Vulnerability and Configuration Management