secpod

TOP VULNERABILITIES REPORT 2021

January to June 2021

www.secpod.com

secpod

TABLE OF CONTENTS

Want to witness the industry's best vulnerability management software live?

Many of the cybersecurity trends that were seen in the last few years have been accelerated by COVID-19, and organizations should take risks seriously. Keeping up with security vulnerabilities is now more crucial than ever. Security threats have surely taken to new heights this year. Ransomware has been the most common and the rising threat trend when it comes to cybersecurity. Inside violations cause 15% to 25% of security breach incidents.

This year, even major security providers experienced targeted attacks. On July 2, Kaseya, an IT solutions provider was attacked and was forced to take its product servers offline. Similarly, in late December 2020, Solarwinds experienced attacks.

Both these attacks caused severe impact on their customers. Being proactive is going to be the most important actions businesses can take in 2021. Organizations who come to terms with the fact that security is no longer an optional investment will more withstand the cybersecurity challenges they now face.

This report is a compilation of the top vulnerabilities found in software pertaining to desktops, laptops, and servers. They may be operating systems, network management applications, and other third-party applications installed in these devices which might have been exposed by the vulnerability.

CRITICAL VULNERABILITIES FROM JANUARY

1. Multiple vulnerabilities in Samba

Description: An unauthenticated attacker on the network can gain administrator access by exploiting a netlogon protocol flaw.

Impact: Exploiting a netlogon protocol flaw.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2020-14318 CVE-2020-14323 CVE-2020-1472	4.3 5.5 10	Samba versions 4.7 and below are affected on Windows, Linux and Mac OS X	Yes

2. Microsoft Defender remote code execution vulnerability

Description: There is a heap buffer overflow when Windows Defender (mpengine.dll) processes the section table when unpacking an ASProtect packed executable.
Each section entry has two values: the virtual address and the size of the section. The code in CAsprotectDLLAndVersion::RetrieveVersionInfoAndCreateObjects only checks if the next section entry's address is lower than the previous one, not if they are equal. This means that if you have a section table such as the one used in this exploit sample: [(0,0), (0,0), (0x2000,0), (0x2000,0x3000)], 0 bytes are allocated for the section at address 0x2000, but when it sees the next entry at 0x2000, it simply skips over it without exiting nor updating the size of the section. 0x3000 bytes will then be copied to that section during the decompression, leading to the heap buffer overflow.

Impact: Leads to heap buffer overflow and remote code execution.

Victims: Proof of this vulnerability being exploited in the wild has been found.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-1647	7.8	Microsoft Windows	Yes

3. Heap-based buffer overflow in Sudo

Description: A flaw was found in sudo. A heap-based buffer overflow was found in the way sudo parses command line arguments. This flaw is exploitable by any local user who can execute the sudo command (by default, any local user can execute sudo) without authentication. Successful exploitation of this flaw could lead to privilege escalation. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Impact: Leads to privilege escalation.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-3156	7.8	Unix and Mac OS X	Yes

CRITICAL VULNERABILITIES FROM FEBRUARY

1. Remote code execution in vCenter/vSphere

Description: Remote code execution vulnerability exists in VMware vCenter/vSphere that allows an unauthenticated attacker to remotely execute code on the VMware hypervisor, where any attacker can upload a code and execute it to control VMware hypervisor.

Impact: Mass scanning activities have been detected. However, there is no proof of exploitation.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-21972	9.8	Unix and Mac OS X	Yes

2. Windows TCP/IP denial of service vulnerability

Description: These vulnerabilities are the result of a flaw in Microsoft's implementation of TCP/IP. Microsoft stated that all three issues could be exploited with a DoS attack and urged customers to install this month's Windows security updates as soon as possible: "We believe attackers will be able to create DoS exploits much more quickly and expect all three issues might be exploited with a DoS attack shortly after release. Thus, we recommend customers move quickly to apply Windows security updates this month. The DoS exploits for these CVEs would allow a remote attacker to cause a stop error. Customers might receive a blue screen on any Windows system that is directly exposed to the internet with minimal network traffic. It is essential that customers apply Windows updates to address these vulnerabilities as soon as possible."

Impact: All three issues could be exploited with a DoS attack, allow a remote attacker to cause a stop error.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-24086 CVE-2021-24094 CVE-2021-24074	7.5 9.8 9.8	Microsoft Windows 7 and above (both Client and Server)	Yes

3. Heap-based buffer overflow vulnerability in Acrobat Reader DC

Description: An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

Impact: Attacker can achieve arbitrary code execution in the context of the current user.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-21017	9.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier)	Yes

CRITICAL VULNERABILITIES FROM MARCH

1. Adobe Creative Cloud improper privilege management privilege escalation vulnerability

Description: This vulnerability allows local attackers to escalate privileges on affected installations of Adobe Creative Cloud on Apple macOS. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.
The specific flaw exists within the Adobe privileged helper tool. The issue lies in the lack of proper validation of the helper clients. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root.

Impact: Escalate privileges on affected installations of Adobe Creative Cloud on Apple macOS

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-21069	7.8	Creative Cloud Desktop Application 5.3 and earlier version on Mac OS X	Yes

2. Adobe FrameMaker PDF file parsing out-of-bounds read remote code execution vulnerability

Description: This vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe FrameMaker. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. Crafted data in a PDF file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.

Impact: Allows remote attackers to execute arbitrary code on affected installations of Adobe FrameMaker.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-21056	7.8	Adobe Framemaker on Windows Versions 2019 Release Update 8 and below and 2020 Release Update 1 and below.	Yes

3. Multiple vulnerabilities in Adobe Photoshop

Description: This vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe FrameMaker. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists within the parsing of PDF files. Crafted data in a PDF file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.

Impact: Execution of code in the context of the current process.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-21056	7.8	Adobe Framemaker on Windows Versions 2019 Release Update 8 and below and 2020 Release Update 1 and below.	Yes

4. Use after free in client_send_params in lib/ext/pre_shared_key.c

Description: It was found that the client sending a "key_share" or "pre_share_key" extension may result in dereferencing a pointer no longer valid after realloc(). This only happens in TLS 1.3 and only when the client sends a large Client Hello message, e.g., when HRR is sent in a resumed session previously negotiated large FFDHE parameters because the initial allocation of the buffer is large enough without having to call realloc().

Impact: A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-20231 CVE-2021-20232	9.8 9.8	gnutls before 3.7.1	Yes

5. fastrpc: restrict user apps from sending kernel RPC messages

Description: It was found that the client sending a "key_share" or "pre_share_key" extension may result in dereferencing a pointer no longer valid after realloc(). This only happens in TLS 1.3 and only when the client sends a large Client Hello message, e.g., when HRR is sent in a resumed session previously negotiated large FFDHE parameters, because the initial allocation of the buffer is large enough without having to call realloc().

Impact: Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-28375	7.8	Linux kernel	Yes

6. Internet Explorer memory corruption vulnerability

Description: A vulnerability in Internet Explorer used in this attack was fixed as CVE-2021-26411. The vulnerability is triggered when users of the affected version of Internet Explorer access a malicious link constructed by attackers.

Impact: Exploitation could cause remote code execution.

Victims: This vulnerability is currently being actively exploited in the wild.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-26411	7.5	Internet Explorer 9 and 11, Microsoft Edge	Yes

7. Windows DNS Server remote code execution vulnerability

Description: CVE-2021-26897 is a DNS server RCE vulnerability, and is triggered when many consecutive Signature RRs Dynamic Updates are sent. This vulnerability is an OOB write on the heap when combining the many consecutive Signature RR Dynamic Updates into base64-encoded strings before writing to the Zone file.

Impact: Exploitation could cause remote code execution.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-26897	9.8	Microsoft Windows Server 2008 and above	Yes

8. Exchange Server SSRF vulnerability

Description: The Microsoft Exchange server attack chain beings with the exploration of this flaw, also known as a server-side-request-forgery (SSRF) vulnerability. When exploited, HTTPS connections are established to authenticate user access. Besides installing all mandatory patches, such untrusted connections can be prevented by placing the Exchange server inside a VPN to separate port 443 from external connection requests.

Impact: Exploitation could lead to malicious code injection and execution.

Victims: This vulnerability is being actively exploited in the wild in masses.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-26855	9.8	Microsoft Windows Server 2013 and above	Yes

9. Buffer overflow in PyCArg_repr in Python

Description: Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.

Impact: Exploitation could allow an attacker to overflow a buffer on the stack and crash the application. The highest threat from this vulnerability is to system availability.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-3177	9.8	Python 3.x through 3.9.1	Yes

10. Xterm flaw allows remote code execution

Description: A missing length check in libX11 causes data from LookupColor requests mess up the client-server communication protocol and inject malicious X server requests. The flaw is comparable to SQLi injecting commands into database connections granting an attacker access to all features of the connection protocol.

Impact: Messes up the client-server communication protocol and inject malicious X server requests.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-3177	9.8	Xterm	Yes

CRITICAL VULNERABILITIES FROM APRIL

1. Win32k elevation of privilege Vulnerability

Description: CVE-2021-28310 is an out-of-bounds (OOB) write vulnerability in dwmcore.dll, which is part of Desktop Window Manager (dwm.exe). Due to the lack of bounds checking, attackers are able to create a situation that allows them to write controlled data at a controlled offset using DirectComposition API. DirectComposition is a Windows component that was introduced in Windows 8 to enable bitmap composition with transforms, effects and animations, with support for bitmaps of different sources (GDI, DirectX, etc.).

Impact: Allows attackers to write controlled data at a controlled offset using DirectComposition API.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-28310	7.8	Microsoft Windows 10 1803 and above	Yes

2. Microsoft Exchange Server remote code execution (RCE) vulnerabilities

Description: Description: CVE-2021-28480 and CVE-2021-28481 are pre-authentication vulnerabilities in Microsoft Exchange Server. A pre-authentication vulnerability means that an attacker does not need to authenticate to the vulnerable Exchange Server in order to exploit the vulnerability. All the attacker needs to do is perform reconnaissance against their intended targets and then send specially crafted requests to the vulnerable Exchange Server.

CVE-2021-28482 and CVE-2021-28483 are post-authentication vulnerabilities in Microsoft Exchange Server. These are only exploitable once an attacker has authenticated to a vulnerable Exchange Server. However, these flaws could be chained together with a pre-authentication Exchange Server vulnerability to bypass that requirement.

Impact: Flaws are exploitable once an attacker has authenticated to a vulnerable Exchange Server. However, these flaws could be chained together with a pre-authentication Exchange Server vulnerability to bypass that requirement.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-28480 CVE-2021-28481 CVE-2021-28482 CVE-2021-28483	9.8 9.8 8.8 9.0	Microsoft Exchange Server 2013 and above	Yes

3. Nettle cryptography library vulnerability

Description: A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation.

Impact: Force an invalid signature, causing an assertion failure or possible validation.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-20305	8.1	Nettle before 3.7.2	Yes

CRITICAL VULNERABILITIES FROM MAY

1. Use after vulnerability in Adobe Reader

Description: This is a zero-day vulnerability in Adobe that was already being exploited in the wild. This exploit allows bad-faith actors to run arbitrary code in the current user context. This means if the users have admin rights, then the code will run with full admin rights.

Impact: Attackers can run arbitrary code in the current user context.

Victims: This vulnerability is currently being actively exploited in the wild.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-28550	8.8	Supported ranges of Adobe Reader on Windows	Yes

2. HTTP Protocol Stack remote code execution vulnerability

Description: The vulnerability allows an unauthenticated attacker to remotely execute code as kernel. This is a wormable vulnerability where an attacker can simply send a malicious crafted packet to the target impacted web-server.

Impact: Allows attacker to remotely execute code as kernel.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-31166	8.8	Microsoft Windows 2004 and higher	Yes

3. Hyper-V remote code execution vulnerability

Description: The vulnerability allows an unauthenticated attacker to remotely execute code as kernel. This is a wormable vulnerability where an attacker can simply send a malicious crafted packet to the target impacted web-server.

Impact: Allows attacker to remotely execute code as kernel.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-28476	9.9	Microsoft Windows Server 2008 and higher	Yes

4. A malicious application may be able to bypass privacy preferences in MacOS Big Sur

Description: A malicious application may be able to bypass Privacy preferences. Apple is aware of a report that this issue may have been actively exploited. The permissions issue was addressed with improved validation.

Impact: Bypass Privacy preferences.

Victims: This vulnerability is being actively exploited by malware.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-30713	Not assigned	Apple Mac OS 11	Yes

5. Multiple vulnerabilities in Pulse Connect Secure 9.1R11.4

Description: Multiple vulnerabilities were discovered and have been resolved in Pulse Connect Secure (PCS). This includes an authentication by-pass vulnerability that can allow an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway. Many of these vulnerabilities have a critical CVSS score and pose a significant risk to your deployment.

Impact: Allow an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway.

Victims: Hackers breached several U.S. federal agencies, critical infrastructure entities, and private entities after exploiting Pulse Connect Secure (PCS) VPN vulnerabilities.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-22893	10	Pulse Connect Secure	Yes
CVE-2021-22899	8.8		
CVE-2021-22894	8.8		
CVE-2021-22900	7.2		

CRITICAL VULNERABILITIES FROM JUNE

1. Remote code execution in Windows MSHTML Platform

Description: The vulnerability allows a remote attacker to execute arbitrary code on the target system.
The vulnerability exists due to a boundary error when processing HTML content within Windows MSHTML Platform. A remote attacker can create a specially crafted web page, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

Impact: Trigger memory corruption and execute arbitrary code on the target system.

Victims: This vulnerability is being actively exploited in the wild.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-33742	8.8	Microsoft Windows 7 and above	Yes

2. Type confusion in V8 in Google Chrome prior to 91.0.4472.101

Description: The vulnerability allows a remote attacker to execute arbitrary code on the target system.
The vulnerability exists due to a boundary error when processing HTML content within Windows MSHTML Platform. A remote attacker can create a specially crafted web page, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

Impact: Trigger memory corruption and execute arbitrary code on the target system.

Victims: This vulnerability is being actively exploited in the wild.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-33742	8.8	Google has released Chrome version before 91.0.4472.101 on Windows, Mac, and Linux	Yes

3. Kerberos AppContainer security feature bypass vulnerability

Description: The vulnerability allows a remote attacker to execute arbitrary code on the target system.
The vulnerability exists due to a boundary error when processing HTML content within Windows MSHTML Platform. A remote attacker can create a specially crafted web page, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

Impact: Trigger memory corruption and execute arbitrary code on the target system.

CVE	CVSSv3 Score	Affected Platforms/Products	Patch Available
CVE-2021-31962	9.8	Microsoft Windows 7 and above	Yes

secpod

Want to witness the industry's best vulnerability management software live?

With the ever-changing IT landscape, a robust and a more comprehensive approach to vulnerability management will help you face vulnerability management challenges easily. SanerNow offers an integrated vulnerability and patch management solution to scan, detect, assess, prioritize, download, test, and also remediate vulnerabilities with automated patching. SanerNow is powered by our homegrown, world's largest SCAP compliant vulnerability intelligence feed with over 130,000 security checks. It also performs the fastest vulnerability scans across all endpoints and network devices within 5 minutes. Sign up for a free demo with us. We'll show what we mean.

Schedule Demo

About SecPod

SecPod is an endpoint management, security, risk, and compliance technology company. SecPod (Security Podium, incarnated as SecPod) has created the revolutionary SanerNow platform and tools that are used by MSPs and enterprises worldwide. SecPod also licenses security technology to top security vendors through its SCAP Content Professional Feed.

Contact Us

www.secpod.com

For enquiries on pricing, email us at: info@secpod.com

Call us at: India - (+91) 80 4121 4020 / USA - (+1) 918 625 3023