ANNUAL VULNERABILITY REPORT 2021

www.secpod.com

SECPOD CYBERHYGIENE REPORT

A story of vulnerabilities, patches, savage hackers and undefeated sysadmins

INDEX

ANNUAL VULNERABILITY REPORT 2021

The digital world has changed, is changing, and will continue to change. The pandemic-led digital transformation and rapid adoption to cloud has brought numerous changes to the IT security landscape. With organization becoming more hybrid, the fight against combatting threats and vulnerabilities has only become more challenging than before. To add to this, the number of vulnerabilities being discovered year after year are only rising above the roof, putting security administrators under constant pressure to manage them. According to the 2021 Hacker-Powered Security Report, organizations has reported over 66,000 valid vulnerabilities this year which is 20% more than the previous one.

Unpatched publicly disclosed vulnerabilities are often the favorite target for attackers. They look out for these open vulnerabilities in the network and create massive security havocs which are hard to deal with. Tightening the security locks and keeping vulnerabilities under check is a huge responsibility for security teams today to keep their digitally-driven businesses running.

From SecPod, we have put together the details of the most critical vulnerabilities of 2021 in this report to keep you aware of the high-risk vulnerabilities and help you protect your network from the wild security storms.

What are the vulnerabilities included in the report?

The report consists of the vulnerabilities possessing high-risks and severity levels from January 2021 to December 2021. The vulnerabilities with the CVSS v3 score of 9.5 and above are included in the report. If you haven't discovered and remediated these vulnerabilities, we strongly recommend that you to get it done immediately

Most Critical Vulnerabilities of 2021

01 Multiple Critical Vulnerabilities In Samba

- **Details of Vulnerability :** The vulnerability can allow an unauthenticated attacker on the network to gain administrator access by exploiting a netlogon protocol flaw.
- **Impact :** Exploiting a netlogon protocol flaw.
- **Patch Availability :** Yes. Samba has released a patch to mitigate this vulnerability.

CVE	CVE-2020-14318 CVE-2020-14323 CVE-2020-14729
CVSSv3 Score	10
Severity	Critical
Affected Product(s)	Samba versions 4.7 and below on Windows, Linux, and Mac OS platforms

02 Critical Remote Code Execution In Vcenter/Vsphere

- **Details of Vulnerability :** 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.

- **Patch Availability :** Yes. VMware has released a patch to mitigate the vulnerability.

CVE	CVE-2021-21972
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	VMware vCenter Server VMware Cloud Foundation

03 Use After Free Vulnerability In client_send_params In lib/ext/pre_shared_key.c

- **Details of Vulnerability :** 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().

- **Patch Availability :** Yes. A Patch is released to fix this issue

CVE	CVE-2021-20231 CVE-2021-20232
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	GnuTLS before 3.7.1

04 Windows DNS Server Remote Code Execution Vulnerability

- **Details of Vulnerability :** CVE-2021-26897 is a DNS server RCE vulnerability 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.

- **Patch Availability :** Yes. A patch is released by Microsoft to remediate this vulnerability.

CVE	CVE-2021-26897
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Microsoft Windows Server 2008 and above

05 Xterm Flaw Allows Remote Code Execution

- **Description:** A missing length checks in libX11 causes data from LookupColor requests to 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.

- **Patch Availability :** Yes. A fix is released by Xterm to remediate this flaw.

CVE	CVE-2021-31535
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Xterm

06 Microsoft Exchange Server Remote Code Execution (RCE) Vulnerabilities

- **Details of Vulnerability :** 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 to exploit the vulnerability. All that 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.

CVE	CVE-2021-28480 CVE-2021-28481 CVE-2021-28482 CVE-2021-28483
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Microsoft Exchange Server 2013 and above

- **Patch Availability :** A patch is released by Microsoft to mitigate this vulnerability

07 HTTP Protocol Stack Remote Code Execution Vulnerability

- **Details of Vulnerability :** 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.

- **Patch Availability :** Yes. A patch is released by Microsoft to mitigate this vulnerability

CVE	CVE-2021-31166
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Microsoft Windows 2004 and higher

08 Hyper-V Remote Code Execution Vulnerability

- **Details of Vulnerability :** 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.

- **Patch Availability :** A patch is released by Microsoft to mitigate this vulnerability

CVE	CVE-2021-28476
CVSSv3 Score	9.9
Severity	Critical
Affected Product(s)	Microsoft Windows Server 2008 and higher

09 Critical Vulnerability In Kaseya VSA Exploited In The Wild

- **Details of Vulnerability :** Kaseya was in the process of fixing various zero-day vulnerabilities reported privately to it, REvil ransomware operators started exploiting the zero-day vulnerabilities to deploy ransomware. Many companies whose networks were managed using Kaseya Virtual System Administrator (VSA) became the victims of this large-scale ransomware attack.

- **Impact :** This has been the largest ransomware attack on record, affecting close to 1500 of Kaseya's clients spread across 17 countries.

CVE	CVE-2021-30116
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Kaseya VSA before 9.5.7

- **Patch Availability :** Yes. 9.5.7 on SaaS Resolving CVE-2021-30116 and CVE-2021-30119.

10 Critical Cisco Router Vulnerabilities

- **Details of Vulnerability :** Cisco Small Business Router (RV340, RV340W, RV345, and RV345P) models running firmware versions earlier than 1.0.03.22 are reported to have contained critical flaws that could be exploited remotely.

  The vulnerabilities with the CVE identifiers CVE-2021-1609 and CVE 2021-1610 reside at the web-based management interface of the Cisco Small Business routers. Specifically, these vulnerabilities stem from improper validation of HTTP requests.

CVE	CVE-2021-1609 CVE-2021-1610
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers

- **Impact :** An unauthenticated, remote attacker could exploit these vulnerabilities to execute arbitrary code or commands using root-level privileges and even cause the device to reload, which will result in a denial of service (DoS) condition.

- **Patch Availability :** Yes. Cisco has released the necessary security updates to address the issue.

11 Improper Input Validation In Node

- **Details of Vulnerability :** Node. js is vulnerable to remote code execution, Cross-site scripting (XSS), and application crashes due to missing input validation of hostnames returned by Domain Name Servers in the Node.js DNS library, leading to the output of wrong hostnames (leading to Domain hijacking) and injection vulnerabilities in applications using the library..

- **Patch Availability :** Yes. Patches are available for v16.x, v14.x, and v12.x Node.js release lines to fix the vulnerability.

CVE	CVE-2021-22931
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Node.js js (<16.6.0, 14.17.4, and 12.22.4)

12 Critical Vulnerability In Atlassian Confluence Server

- **Details of Vulnerability :** An OGNL injection vulnerability exists that allows an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance.

- **Patch Availability :** Yes. Atlassian Confluence server has released patches to fix the vulnerability.

CVE	CVE-2021-26084
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Confluence Server and Data Center multiple versions

13 Critical Zero-Day Vulnerability In Zoho's ADSelfService

- **Details of Vulnerability :** The vulnerability can be triggered by sending a specially crafted request to the REST API endpoint of ADSelfService plus. As a result, an attacker can perform unauthenticated RCE on the affected systems.

- **Patch Availability :** Yes. Zoho has released a fix for this vulnerability.

CVE	CVE-2021-40539
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Zoho ManageEngine ADSelfService Plus version 6113

14 ap_escape_quotes() May Write Beyond The End Of A Buffer When Given Malicious Input

- **Details of Vulnerability :** An out-of-bounds write in function ap_escape_quotes of httpd allows an unauthenticated remote attacker to crash the server or potentially execute code on the system with the privileges of the httpd user by providing malicious input to the function.

- **Patch Availability :** Yes. A patch is available to fix this vulnerability.

CVE	CVE-2021-39275
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Apache HTTP Server 2.4.48 and earlier

15 Critical Remote Code Execution Vulnerability In Zoho ManageEngine Desktop Central

- **Details of Vulnerability :** An authentication bypass vulnerability in ManageEngine Desktop Central was identified and the vulnerability can allow an adversary to bypass authentication and execute arbitrary code in the Desktop Central server.

- **Patch Availability :** Yes. A fix has been released by Zoho to address this vulnerability

CVE	CVE-2021-44515
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	Zoho ManageEngine Desktop Central multiple versions

16 Critical Vulnerability In Mozilla's Cryptographic Library

- **Details of Vulnerability :** NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS.

- **Patch Availability :** Yes. Mozilla has released a patch to address this vulnerability

CVE	CVE-2021-43527
CVSSv3 Score	9.8
Severity	Critical
Affected Product(s)	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR

17 Critical Vulnerability In Mozilla's Cryptographic Library

- **Details of Vulnerability :** Remote code execution in Log4j 2.x when logs contain an attacker-controlled string value. A flaw was found in the Apache Log4j logging library in versions from 2.0.0 and before 2.15.0. A remote attacker who can control log messages or log message parameters can execute arbitrary code on the server via JNDI LDAP endpoint.

  This issue only affects log4j versions between 2.0 and 2.14.1. In order to exploit this flaw you need:
  - A remotely accessible endpoint with any protocol (HTTP, TCP, etc) that allows an attacker to send arbitrary data
  - A log statement in the endpoint that logs the attacker-controlled data.

CVE	CVE-2021-44228
CVSSv3 Score	10
Severity	Critical
Affected Product(s)	Apache Log4j logging library in versions from 2.0.0 and before 2.15.0

- **Impact :** The log4j vulnerability **allows attackers to execute malicious code remotely on a target computer.** This can allow hackers to easily steal data, install malware, or simply take control of a system via the Internet.

- **Patch Availability :** Yes. Apache has released a patch to fix this vulnerability

SecPod SanerNow’s Full-fledged Vulnerability Management for the New Digital Era

The Pandemic which hit us is 2020 does not seem to settle. The IT security landscape will only keep evolving more to meet the expectations of the changing digital era. The vulnerability attack surface will continue to expand, and conventional vulnerability management methods will not suffice in the on-going trend.

SecPod SanerNow offers a full-fledged solution for continuous and automated vulnerability management. It can help you:

- Run continuous and automated vulnerability scans in less than 5 minutes
- Detect vulnerabilities accurately leveraging the world’s largest vulnerability database
- Assess and prioritize vulnerabilities based on severity level
- Remediate vulnerabilities on time with integrated patch management
- Execute other critical cyber hygiene measures to achieve seamless security

Yes

Schedule Demo

We will show you a modern approach to manage vulnerabilities!

Assets Based On Publisher

+ Adobe systems Incorporated	3
+ Martin Prikryl	1
+ SecPod Technologies	3
+ Cisco Webex LLc	9
+ Adobe	3
+ Adobe systems	3

About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on the computing environment. Our product helps implement cyber hygiene measures, so attackers have a tough time piercing through.

Our SanerNow CyberHygiene platform is a continuous and automated vulnerability management solution. It provides continuous visibility to the computing environment, identifies vulnerabilities and misconfigurations, mitigates loopholes to eliminate attack-surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better every day.

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