# 2021 Red Hat Product Security risk report

**2021 at a glance:**

1,473 CVEs were addressed throughout 2021, a 28% decrease from 2020.

1,385 Red Hat Security Advisories were issued, a slight decline from 2020.

46 Critical advisories addressed 10 Critical vulnerabilities.

50% of Critical issues were addressed within one business day, an improvement from 2020.

83% of Critical issues were addressed within one week, in line with last year.

22% of Important issues were addressed within one business day, exceeding last year.

33% of Important issues were addressed within one week, exceeding our pace in 2020.

57% of Important issues were addressed within 31 days, slightly behind 2020's delivery.

## Introduction

The 2021 edition of the Red Hat Product Security risk report is an overview of security vulnerabilities that affected Red Hat® products for the calendar year. Along with reporting the vulnerabilities that affected our products we highlight the major incidents and note Red Hat's response to these issues.

Red Hat assigns Common Vulnerabilities and Exposures (CVE) identifiers to every new security issue. Each vulnerability receives a score based on the Common Vulnerability Scoring System (CVSS) version 3. Red Hat Product Security also assigns a severity rating to each identified vulnerability. We make all of this information publicly available with the goal of helping our users better understand these issues.

True to Red Hat's open source heritage, Red Hat's Product Security and Incident Response teams operate with the belief that openly sharing information, contributing our knowledge, and collaborating to solve issues can result in better outcomes faster—not only for Red Hat customers but for the industry as a whole.

This open source spirit has earned us trust from Red Hat customers, upstream communities, and across the IT industry. Red Hat Product Security supports both Red Hat's engineering needs and upstream communities, as well as a broader IT ecosystem that relies on our analysis and information to assess their systems and environments more quickly. This community-minded ethos inspires us to continue delivering positive customer experiences, engagement, and proactive solutions.

Along with a commitment to open source principles, Red Hat is committed to our customers and the security of our offerings. In Product Security, this commitment is evidenced by the volume of issues we address and by delivering responses that give our customers and partners confidence in Red Hat.

## Four major security bulletins of 2021

Red Hat strives to provide top customer value and support, including helping our customers manage risks associated with major vulnerabilities via Red Hat Security Bulletins. Some of the major vulnerabilities we addressed in 2021 include:

- Apache Log4Shell
- DNSpooq
- Sudo privilege escalation
- Trojan source attacks

Red Hat Security Bulletins contain the most current information on new vulnerabilities, diagnostic tools, and updates and fixes for new product releases. Customers can use this information to make risk-based decisions on their environment.

For a list of all major security incidents, visit the Security Bulletins page.

### Red Hat Security Bulletin #1: Apache Log4Shell vulnerability

The Log4Shell (CVE-2021-44228) vulnerability shook the IT world at the end of 2021. This Critical security flaw allowed attackers to easily compromise vulnerable application services with a simple malicious code attack using injection tactics.

The Log4Shell vulnerability was one of the most severe vulnerabilities in the history of information security. The severity of this vulnerability was due to the widespread use of the Log4J tool and the simplicity of the attack.

Java(TM) is in many digital systems, front ends, products, appliances, and services. When a Java program needs logging, the Log4J tool is a widely used solution. This vulnerability could easily affect most Java software that made use of Log4J. This flaw affected all versions of Log4J version 2 prior to version 2.15.0.

While the initial Log4Shell was indeed a critical issue, there were seven different Log4J vulnerabilities discovered after the initial CVE was reported. These additional vulnerabilities also affected Log4J version 1, which the Apache Software Foundation stopped supporting seven years ago.

Red Hat delivered Critical CVE updates for affected products in three business days, addressing the issue more quickly and accurately. Red Hat also treated the seven subsequent vulnerabilities across multiple products and versions as part of the major security incident, regardless of the severity levels assigned to the subsequent CVEs, and provided patches for Log4J version 1. All patches shipped by Red Hat are fully supported.

### Red Hat Security Bulletin #2: DNSpooq

Dnsmasq, a DNS and DHCP toolbox software widely used within specific virtual environments and in small networks, was affected by seven security issues (CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687), branded collectively as DNSpooq.

Moshe Kol and Shlomi Oberman from JSOF discovered the vulnerabilities. Red Hat, CERT/CC, Cisco, Google, and the Pi-Hole incident response teams supported the disclosure coordination and the release of vulnerability information.

This vulnerability affected the following Red Hat products:

- Red Hat OpenStack® Platform 10
- Red Hat OpenStack Platform 13
- Red Hat Virtualization 4.3
- Red Hat Virtualization 4.4
- Red Hat OpenShift® Container Platform 3.11
- Red Hat Enterprise Linux® 7
- Red Hat Enterprise Linux 8

A remote attacker could execute code on the victim machine through one of two vulnerabilities: CVE-2020-25681 and CVE-2020-25682. The other vulnerabilities allowed the execution of a DNS cache poisoning attack. Red Hat analyzed the attack surface and the component usage in each affected product to rate the vulnerability. This consideration provided precise information for our customers, such as mitigations that they could apply in affected products to reduce or eliminate the risk introduced by these flaws.

### Red Hat Security Bulletin #3: Sudo privilege escalation vulnerability

Another vulnerability that received a high level of attention in January 2021, was a sudo flaw (CVE-2021-3156) that was originally introduced in July 2011.

The attacker could cause memory corruption by exploiting a faulty parsing of command-line parameters, leading to a crash or privilege escalation. An attacker needs local shell access to the system to exploit this vulnerability.

Because the sudo package is installed by default on all Red Hat Enterprise Linux systems and allows users to execute commands as other users, most commonly root, Red Hat Product Security has classified this flaw as having a severity rating of Important. Red Hat provided a systemtap-based mitigation and quick updates for our potentially affected products within the Red Hat portfolio.

The sudo flaw potentially affected the following Red Hat product versions and containers:

- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- Red Hat OpenShift Container Platform 4
- Red Hat Virtualization 4.3 and 4.4
- Red Hat OpenShift Container Storage 4
  - ocs4/rook-ceph-rhel8-operator
  - ocs4/cephcsi-rhel8

### Red Hat Security Bulletin #4: Trojan source attacks

In late 2021, Red Hat published a Security Bulletin on the Trojan source attacks (CVE-2021-42694), also known as BiDi. This issue introduced a new source code and supply chain attack scenario, where the behavior of the software and the expectations from the source code do not match. In this attack, source code reviewed by a human would be different from the software, which is generated by the compiler.

Red Hat led a massive disclosure coordination effort between several Linux distributions, upstream projects, and standard working groups. We discussed the scope of the vulnerability, shared and worked on our scanning and detection script with them, and helped design patches for the issue.

Red Hat not only scanned our codebase and internal infrastructure, but for the first time, we also made our detection script available on GitHub for community collaboration. Other Linux distributors and several upstream projects used this detection script to scan their code and within their CI/CD pipelines. Red Hat also led efforts to fix the GNU Compiler Collection (GCC) to detect special characters in code and coordinate with other language projects.

## Vulnerability trends

In 2021, the entire software industry experienced changes that resulted in significant security impacts, including supply chain attacks and ransomware incidents. These security events prompted a worldwide response, including government-issued executive orders and increased customer attention on supply chain reviews and responses. Red Hat is deeply committed to software supply chain security. The improvements we made in the last year and increased scrutinization of software security contributed in a noteworthy way to the decrease in vulnerabilities in 2021.

### Red Hat Security Advisories and CVEs

Red Hat Security Advisories and CVEs showed different trends in 2021 compared to previous years. For example, the number of reported CVEs was 22% lower than 2020, and the number of Red Hat Security Advisories was also lower than the previous year.

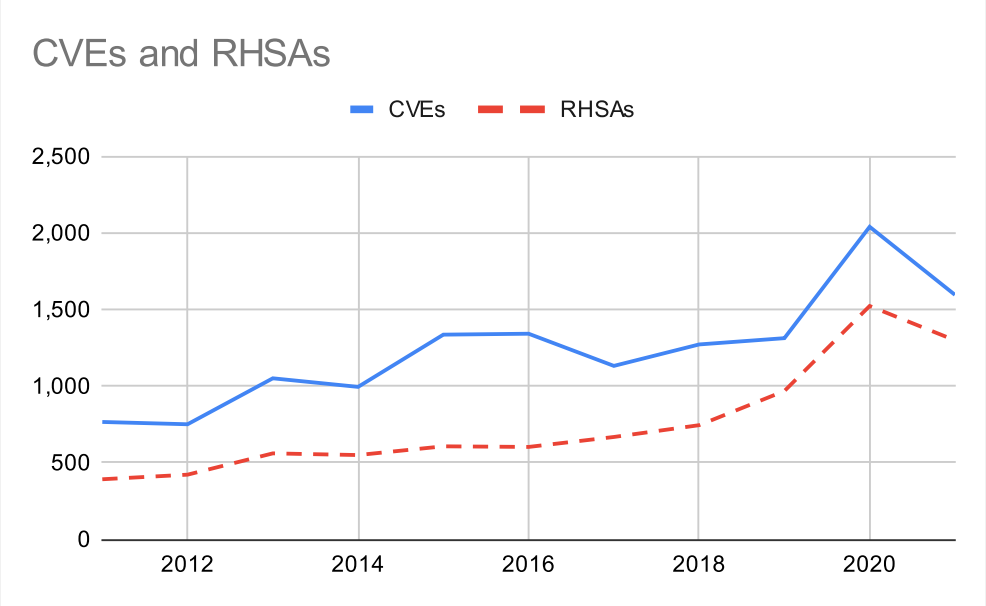


Figure 1. CVEs, and Red Hat Security Advisories

### CVEs by severity for all Red Hat offerings

Between 2020 and 2021, CVEs decreased for all severity ratings. One significant trend across the past five years is a decrease in the average incidence of Critical CVEs with an 80% departure from the trailing five-year average. A combination of factors focusing on layered products, security-focused development, and upstream package reviews have resulted in this significant decrease of vulnerabilities.

Red Hat will continue this work to reduce the severity and number of CVEs improving the maturity of our offerings using our Secure Software Management Life Cycle (SSML) implementation of the NIST Secure Software Development Framework (SSDF) during the development process.

**Table 1. CVEs for all Products: Five-Year Trend**

| Year | Low | Moderate | Important | Critical |
|---|---|---|---|---|
| 2017 | 183 | 576 | 247 | 126 |
| 2018 | 298 | 649 | 268 | 57 |
| 2019 | 281 | 665 | 340 | 27 |
| 2020 | 460 | 1,136 | 425 | 19 |
| 2021 | 243 | 1,060 | 283 | 10 |

Red Hat rates the severity of CVEs as Low, Moderate, Important, and Critical. The majority of CVEs in 2021 were Moderate. Less than 1% of all Red Hat reported security issues had a Critical security rating and less than 20% had an Important severity rating.

To learn more about severity rating, see Understanding Red Hat severity ratings.

### Red Hat Security Advisories in 2021

Red Hat Security Advisories—ranked as Low, Moderate, Important, or Critical based on the highest security rating of the vulnerabilities fixed in the advisory—contain one or more security fixes and may also contain bug or enhancement fixes. For many organizations, Red Hat Security Advisories are Red Hat's most important type of errata. The decrease of severe vulnerabilities reflects in less downtime, maintenance windows, change management meetings, and costs to the user. Customers are now able to use fewer resources to review vulnerabilities and patch their environments.

**Table 2. Red Hat Security Advisories severity count trend**

| Product | Critical | Important | Moderate | Low |
|---|---|---|---|---|
| All | 46v | 708v | 582v | 63v |
| Red Hat Enterprise Linux 7, 8 | 27v | 551v | 317v | 30v |
| Red Hat Enterprise Linux 7—default install | 4v | 83v | 29v | 2v |
| Red Hat Enterprise Linux 8—default install | 5v | 135^ | 175^ | 23v |
| Red Hat JBoss® Enterprise Application Platform—all supported versions | 0v | 16v | 22^ | 1^ |

| Product | Critical | Important | Moderate | Low |
|---|---|---|---|---|
| Red Hat OpenShift—all supported versions | 9^ | 61v | 119v | 12v |
| Red Hat OpenStack Platform—all supported versions | 0-- | 12v | 11v | 0v |

*Legend (2020 comparison)*

*^ = trend up*

*v = trend down*

*-- = no trend*

### Red Hat Security Advisories and CVEs: Resolution in days

For flaws rated Critical or most severe, Red Hat responded within five days on average. The median day response for these vulnerabilities was four days. For flaws rated Important, Red Hat responded within 61 days on average. The median day response for these vulnerabilities was 25 days.

### Table 3. Red Hat Security Advisories and CVEs

| Year | Avg (Critical) | Median (Critical) | Avg (Important) | Median (Important) |
|---|---|---|---|---|
| 2015 | 1 | 1 | 31 | 5 |
| 2016 | 2 | 1 | 32 | 6 |
| 2017 | 2 | 1 | 43 | 4 |
| 2018 | 18 | 3 | 61 | 7 |
| 2019 | 7 | 3 | 70 | 23 |
| 2020 | 6 | 4 | 59 | 16 |
| 2021 | 5 | 4 | 61 | 5 |

Red Hat Enterprise Linux accounts for two-thirds of the Critical vulnerabilities we addressed in 2021. This table is based on the number of components included in this product.

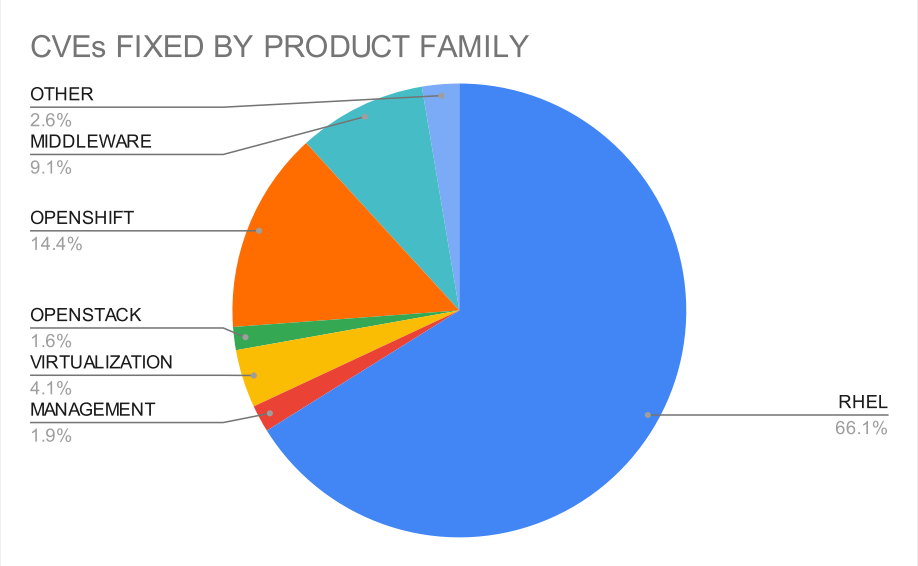


Figure 2. CVEs fixed by product family

## Default installation of Red Hat products

The default configuration of all Red Hat products comes in a hardened state that covers the majority of possible use cases. In addition, customers can remove packages they do not need for their day-to-day operations to reduce potential threats.

It is worth noting that when default security features like SELinux are disabled, the risk profile of that system is drastically altered, opening up the potential for additional security risks and impacts.

**Table 4. Red Hat offering package counts**

| Product | Number of packages |
|---|---|
| Red Hat Enterprise Linux 8.5 Server (minimal) | 390 RPMs |
| Red Hat Enterprise Linux 8.5 Workstation (default w/GUI) | 1,385 RPMs |
| Red Hat OpenStack Platform 16.2 | 805 RPMs + underlying operating system (OS) |
| Red Hat OpenShift Container Platform 4.9 | 34 containers + underlying OS |
| Red Hat JBoss Enterprise Application Platform 7.4.2 | 1,039 jars + underlying OS |
| Red Hat Satellite 6.10 (on Red Hat Enterprise Linux 7 x86_64) | 491 Core packages + 261 Satellite Capsule packages + 60 Satellite Tools packages + underlying OS |

## Known exploits of vulnerabilities in 2021

Known exploits received far more attention in 2021 than in previous years. To improve our workflows and learn more about potential risks to our customers, we looked into available data in the industry, including resources from the Cybersecurity and Infrastructure Security Agency (CISA, part of the U.S. Department of Homeland Security), The Exploit Database (a project sponsored by Offensive Security), and Metasploit.

Red Hat reported 1,596 CVEs affecting our products in 2021. When broken down by impact, we saw the following: 10 Critical, 283 Important, 1,060 Moderate, and 243 Low. Of these, only 26 or 1.6% of all CVEs affecting Red Hat products have known exploits, at the time of this writing. This value is below the industry average of 4%.

**Table 5. Known exploits of 2021**

| Severity | CVEs | Exploits | Percentage |
|---|---|---|---|
| Critical | 10 | 1 | 10.0% |
| Important | 283 | 7 | 2.5% |
| Moderate | 1,060 | 18 | 1.7% |
| Low | 243 | 0 | 0.0% |
| All | 1,596 | 26 | 1.6% |

On average, it took three months for an exploit to be publicly available after reporting the CVE. However, in a few rare high-profile cases, such as Log4Shell, the exploit was available immediately when the vulnerability was made public. Customers must update vulnerable software as soon as possible. It is also imperative to use preventive security measures, such as SELinux, which is often effective against 0-day vulnerabilities.

Red Hat fixed every Critical and Important CVE with exploits for all supported products. We also fixed all Moderate CVEs with exploits for all supported products, except one issued for an already deprecated package.

In 2022, we plan to integrate exploit data into more parts of our vulnerability management process. This will allow us to more quickly and accurately protect our customers and provide easily accessible information about potential risks posed by known exploits.

### Most viewed CVEs in 2021

In 2021, CVE-2021-3156 was our most viewed CVE, receiving almost 10 times the number of views of any other 2021 CVE. Eight out of 10 of our most viewed CVEs dealt with OpenSSL or the Linux kernel. Red Hat will continue monitoring these trends throughout 2022.

| CVE | | | |
|---|---|---|---|
| ID | Severity | Title Text | Pageviews |
| CVE-2021-3156 | Important | sudo: Heap buffer overflow in argument parsing | 195,920 |
| CVE-2021-3449 | Important | openssl: NULL pointer dereference in signature algo.. | 20,952 |
| CVE-2021-3450 | Important | openssl: CA certificate check bypass with X509_V_FL.. | 16,706 |
| CVE-2021-27365 | Important | kernel: heap buffer overflow in the iSCSI subsystem | 10,972 |
| CVE-2021-23840 | Moderate | openssl: integer overflow in CipherUpdate | 10,330 |
| CVE-2021-3177 | Moderate | python: buffer overflow in PyCArg_repr in _ctypes/c.. | 10,176 |
| CVE-2021-23841 | Moderate | openssl: NULL pointer dereference in X509_issuer_a.. | 9,804 |
| CVE-2021-3347 | Important | kernel: Use after free via PI futex state | 7,800 |
| CVE-2021-27364 | Important | kernel: out-of-bounds read in libiscsi module | 7,464 |
| CVE-2021-27363 | Moderate | kernel: iscsi: unrestricted access to sessions and han.. | 7,130 |

Figure 3. Most viewed 2021 CVEs in 2021

## Looking ahead

Red Hat continues to have a dedicated focus on helping our customers manage security risks. To do this, we use early coordination and engagement that involves clear analysis and recommendations to address vulnerabilities that affect our software offerings more quickly.

Risk is all about context and appears differently depending on your system and environment. At Red Hat, our incident response process allows us to provide a response with useful data to combat the threats and vulnerabilities that affect your organization.

The total number of CVEs reported is at 1,596, which is the same approximate level for the past five years, and the percentage of exploitation remains relatively low at 1.6% overall. Critical issues were lower as well from the past years.

Further, we are excited about upcoming releases in community work regarding CVE and the provisioning of more complete data and automation later this year. This impending release involves rolling out new versions of CVE JSON5 and Services 2.1.1 this spring. Red Hat is already releasing this information after much testing and significant contributions throughout the process. The expected results are better updates to CVE metadata in a more timely and automated fashion to the National Vulnerability Database (NVD) for users.

For more information about our vulnerability management process, we invite you to read An open approach to vulnerability management.

For the latest information on security for Red Hat products and services, please visit Red Hat Product Security Center.

## About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

**North America**
1 888 REDHAT1

**Europe, Middle East, and Africa**
00800 7334 2835
europe@redhat.com

**Asia Pacific**
+65 6490 4200
apac@redhat.com

**Latin America**
+54 11 4329 7300
info-latam@redhat.com



redhat.com
#F31254_0322