RED HAT PRODUCT SECURITY RISK REPORT: 2017

This report explores the state of security risk for Red Hat® products for calendar year 2017. We review key metrics, specific vulnerabilities, and the most common ways users of Red Hat products were affected by security issues.

TABLE OF CONTENTS

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

redhat.com

COMMON VULNERABILITIES AND EXPOSURES (CVES)

Every security issue addressed by Red Hat will have a Common Vulnerabilities and Exposures (CVE) identifier associated with it. If we fix a bug that later turns out to have contained a security vulnerability, we retroactively assign the issue a CVE identifier. Every CVE fixed has an entry in our public CVE database in the Red Hat Customer Portal as well as a public bug that has more technical detail. For the purposes of this report, we use the terms "vulnerability" and "CVE" interchangeably.

Note: Because assigning and reporting practices vary considerably between vendors, users are cautioned when comparing reports to ensure they fully understand the CVE evaluation methodologies, assigning practices, and reporting processes for each vendor. Even two Linux vendors may have counts and numbers that seem starkly different simply because the same CVE is mitigated differently in each product build or the integration thereof.

In 2017, across all Red Hat products, and for all issue severities, we addressed more than 980 vulnerabilities and released more than 670 security advisories. For any given organization, only a subset of those issues could be applicable for the products and versions in use.

Red Hat Product Security rates each vulnerability using a four-point scale (Low, Moderate, Important, or Critical) to prioritize and categorize each security issue. Each customer's risk posture and environment is unique, and severity levels are only one way we help our customers understand their exposure. With a comprehensive understanding of the vulnerability, our customers can then review their own threat models and risk postures, and make a more informed business decision on scheduling upgrades to their systems.

We also publish Common Vulnerability Scoring System (CVSS) scores for every vulnerability addressed. This helps customers who use CVSS scoring for their internal processes. Red Hat started using CVSS v3.0 scoring during 2016 and at the start of 2017 it became our default version. CVSS is one of many factors Red Hat uses to evaluate and prioritize vulnerabilities.

To better understand how Red Hat uses the CVSS v3.0 scoring methodology, read our blog post, "How Red Hat Uses CVSSv3 to Assist in Rating Flaws" or review this solution article, "CVSS v3.0 Base Metrics," which provides examples of how base metrics between organizations differ.

Vulnerabilities rated Critical in severity can pose the most risk to an organization. By definition, a Critical vulnerability is one that could potentially be exploited remotely and automatically by a worm. Red Hat, like other vendors, expands the definition to include those flaws that affect web browsers or plug-ins where a user only needs to visit a malicious (or compromised) website in order to be exploited. If you're using a Red Hat product that does not have a desktop, you'll be affected by significantly fewer Critical vulnerabilities.

VULNERABILITY TRENDS

BY THE NUMBERS

For those readers who are new to vulnerability management, trying to understand how many CVEs there are in a product can be a challenge. The most important concept to grasp when "counting" CVEs is that it is not a 1:1 ratio of CVE-to-product when it comes to Red Hat technology, as one advisory can address multiple CVEs.

For example, if you visit the security advisories page, you can find the last publicly released Critical advisory of 2017, RHSA-2017:3401, which addressed 19 CVEs. As a general rule, a count of vulnerabilities can be used as an estimate of the amount of effort required to understand the issues and fixes, whereas a count of advisories can be used as an estimate of the amount of effort to deploy updates.

From an overall risk perspective, in 2017 we saw more security errata released than previous years, and a reduction in the number of flaws addressed by them. The data seen in charts 1 and 2 is available for our customers using the daysofrisk.pl script available on our Security Metrics page. The numbers seen in chart 3 represent the number of flaws fixed in our supported products.

In addition to the daysofrisk.pl script, the Security Metrics page provides the following to facilitate tracking and mapping of vulnerability data:

- Common Vulnerability Reporting Framework (CVRF) documentation
- OVAL definitions are available for vulnerabilities that were addressed in errata for Red Hat Enterprise Linux 3, 4, 5, 6, and 7
- CVE to date, CVE to severity, and CVE to CVSS mapping
- Red Hat Security Advisories to date and times the advisories were issued
- CVE to CWE mapping
- RPM to CVE mapping
- Lists of packages in default installations, which can be used to filter the metrics available from the scripts provided

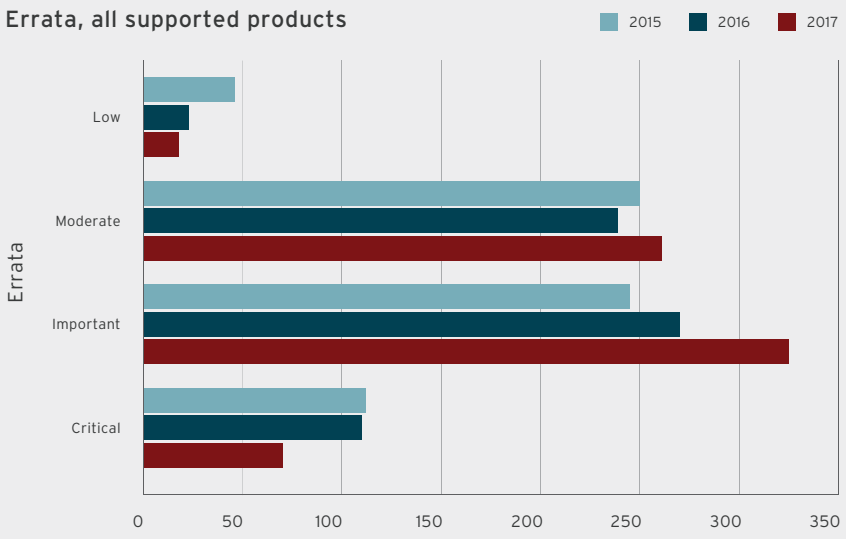


Figure 1. Vulnerabilities in all supported products from 2015-2017

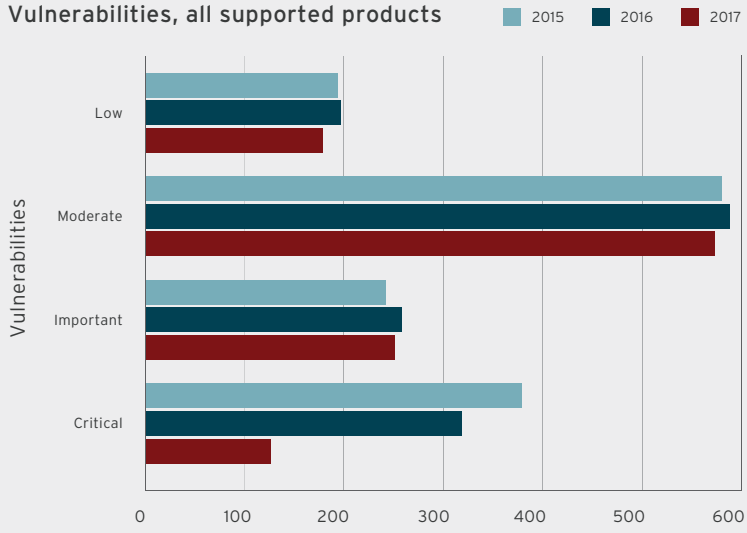


Figure 2. Vulnerabilities in all supported products from 2015-2017

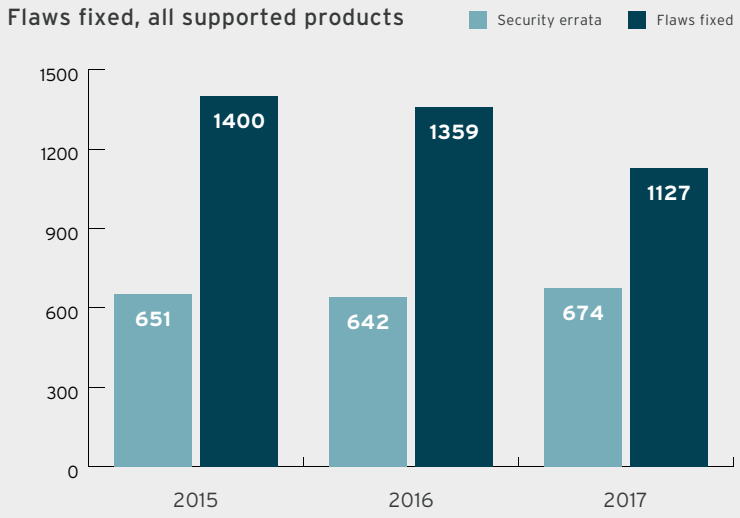


Figure 3. Flaws fixed in all supported products from 2015-2017

Tables 1-3 reflect the 2017 vulnerability counts for a selected subset of product families: RHEL 5, 6, 7, and their supported streams.

Because one CVE can affect multiple supported versions of the same product, we do not total the criticality columns vertically, as that could result in the same CVE being counted twice and would not accurately represent the total count. Instead, we tally them across the table to accurately reflect the number of CVEs that apply to each specific product version.

TABLE 1. RED HAT ENTERPRISE LINUX 5

PRODUCT	CRITICAL	IMPORTANT	MODERATE	LOW	TOTAL
RHEL 5	12	8	20	4	44
RHEL 5 Extended Lifecycle Support	2	6	1	1	10
RHEL 5 Long Life	0	2	0	0	2
RHEL 5 Optional Productivity Applications	8	0	8	1	17

TABLE 2. RED HAT ENTERPRISE LINUX 6

PRODUCT	CRITICAL	IMPORTANT	MODERATE	LOW	TOTAL
RHEL 6	41	89	124	30	284
RHEL 6 Supplementary	83	75	84	30	272

TABLE 3. RED HAT ENTERPRISE LINUX 7

PRODUCT	CRITICAL	IMPORTANT	MODERATE	LOW	TOTAL
RHEL 7	45	124	257	66	492
RHEL 7 Extras	0	0	2	1	3
RHEL 7 for Real Time	0	14	24	2	40
RHEL 7 Supplementary	14	7	26	4	51

The number of vulnerabilities addressed by Red Hat year over year generally increases as a function of new products being continually released, although the numbers were similar between 2015, 2016, and 2017. When looking at a specific product, we find that the number of vulnerabilities being fixed decreases over time because of our security fix backporting policies. Additionally, the number of flaws we fix is reduced when we have products that reach their end of life (EOL).

Backporting is the process in which we take a fix for a security flaw out of the most recent version of an upstream software package, and apply that fix to an older version of the package we distribute. Backporting is an essential part of deploying automated updates to customers with minimal risk.

RED HAT RESPONDS TO CVEs

Not all CVEs are created equal. Red Hat reviews a large number of CVEs each year and 2017 was packed full of vulnerability analysis by Red Hat Product Security. As is our customary practice, we track and review every CVE we receive.

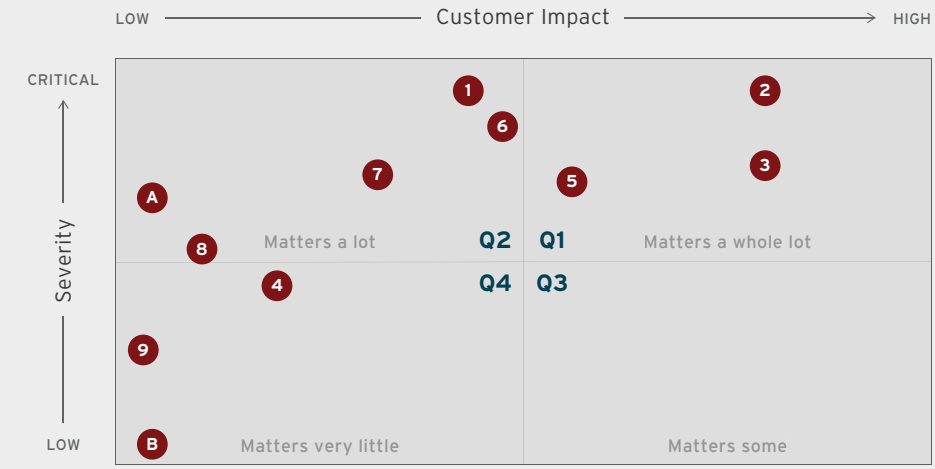
Red Hat strives to release product-related vulnerability information, fixes, and related mitigations to our customers as quickly as possible. However, sometimes upstream communities release fixes without recognizing or specifying that the fix is relevant to security; this may have been the case in CVE-2017-6056. We saw this CVE released in February, but the upstream apache bug was made public in 2015. This means that, while there were 767 days of public exposure where customers were vulnerable, there were approximately 20 days of exposure from when Red Hat first found out about the issue.

In 2017, we responded to almost 1,000 CVE notifications and in many cases had a fix and security advisory published the same day the CVE was made public. This means patches were immediately available for customers.

- 70 Critical advisories addressing 126 Critical vulnerabilities
- 73% Critical issues addressed next business day
- 96% Critical issues addressed within one week

DETERMINING ISSUES THAT MATTERED IN 2017

NOTES: https://access.redhat.com/security/vulnerabilities



1 - *Solr/Lucene (CVE-2017-12629)*
2 - Dnsmasq
3 - *KRACK (CVE-2017-13077)*
4 - CVE-2017-7200
5 - Dirty COW Variant
6 - *Blueborne (CVE-2017-1000251)*
7 - *SambaCry (CVE-2017-7494)*
8 - *Systemd (CVE-2017-9445)*
9 - CVE-2017-9804
A - CVE-2017-9805
B - CVE-2017-6451

Figure 4. Four-quadrant severity map

The issues in this section were included based on what quadrant they fell into. When deciding what really matters, we consider two factors: the severity of the CVE, and the impact on our customer.

Each customer is unique, and they may not be targeted in the same way. In some cases, a customer may determine that a Low-severity vulnerability with no exploit matters because of who they believe is targeting them, and what threat they believe the actor poses based on their threat models. Thus, we recommend all customers carefully review each vulnerability within the context of their threat models to accurately determine their unique risk.

Red Hat uses a four-point scoring system to determine the severity of any given vulnerability. Red Hat's scoring system parallels the vendor-agnostic National Vulnerability Database (NVD) scoring system. One distinct difference between our scoring systems is that we use a qualitative predefined scoring system, while NVD uses a numerical scoring system.

Although we did not have any branded CVEs until the latter half of the year, there were many that were important to our customers throughout the entire year. Based on customer feedback, interactions with Red Hat Technical Account Management, and the number of visits to CVE pages, we've selected the top five CVEs that generated the most discussion, and consolidated them in table 4.

TABLE 4. TOP 5 CVEs OF 2017

CVE & DESCRIPTION	DAYS EMBARGOED	DAYS TILL FIRST ERRATUM	# OF ERRATA	CVSS SCORE	IMPACT
CVE-2017-1000364 kernel: heap/stack gap jumping via unbounded stack allocations	40	0	13	7.4	Important
CVE-2017-7494 Samba: Loading shared modules from any path in the system leading to RCE (SambaCry)	15	0	5	7.5	Important
CVE-2017-1000253 kernel: load_elf_ binary() does not take account of the need to allocate sufficient space for the entire binary	11	0	10	7.8	Important
CVE-2017-1000367 sudo: Privilege escalation in via improper get_process_ ttyname() parsing	8	0	2	7.8	Important
CVE-2017-6074 kernel: use after free in dccp protocol	5	0	15	7.8	Important

Of these top five, the top three had very small margins separating them, and none of them needed a catchy name to get our attention. Below we look at each of them in a little more detail.

CVE-2017-1000364 (Red Hat impact score: Important)

Days embargoed: **5**
Days from public notification to patch release: **0**
Total errata released: **13**

Coming in at the top of the list for customer interest, CVE-2017-1000364 was made public on 2017-06-19. This vulnerability in the Linux kernel affected many Linux vendors including Red Hat. Specific platform information can be found in the Red Hat CVE database. This particular kernel vulnerability affects an almost-five-year-old kernel, versions 4.11.5 and earlier, with stack guard enabled. It's fairly simple to exploit on a program with any sort of controllable state. If exploited, it was evaluated (on the CVSS v3.0 scoring system) as having a potentially high impact on confidentiality, integrity, and availability of a host.

CVE-2017-7494 (Red Hat impact score: Important)

Days embargoed: **12**
Days from public notification to patch release: **0**
Total errata released: **5**

Made public on 2017-05-24, this CVE generated the second-highest level of customer interest. Because of our relationships with open source communities, we learned about the flaw from our upstream developers before it was made public, allowing us ample time to identify mitigations. This Samba-related vulnerability sparked an almost equal level of interest as the most interesting vulnerability for our customers, and was also evaluated as having a potentially high impact on the confidentiality, integrity, and availability of a host. With a network attack vector (versus a local one as with the previous CVE), and the potential for remote code execution, this gained considerable attention among technical audiences.

Customers may have noted that our CVSS v3.0 score for this vulnerability was 7.5 rather than the 9.8 NVD assigned. The reason for this is that the related platforms ship with SELinux turned on by default. When run in enforcing mode, our default policy prevents loading of modules from outside of Samba's module directories and therefore prevents exploitation.

Because this issue could be mitigated by SELinux (enabled by default) and this flaw required the Samba server to be configured in a nonstandard way, our scoring of the vulnerability using CVSS v3.0 metrics rated the "Attack Complexity" as High (AC:H) instead of Low. We rated "Privileges Required" as Low (PR:L) because we assume Samba is deployed requiring authentication for clients.

NVD NIST assumes the worst-case scenario, where Samba is configured having anonymous write access to a share. Such configuration is the opposite of good security practices. Being more difficult to exploit and requiring at least some privileges, this vulnerability in our software was a lower risk than other platforms running affected versions of the Samba code.

Additionally, there were two other mitigations available to our customers, and you can read about them in the Red Hat CVE database.

CVE-2017-1000253 (Red Hat impact score: Important)

Days embargoed: **11**
Days from public notification to patch release: **0**
Total errata released: **10**

Made public on 2017-09-26, this CVE is concerned with the way in which the Linux kernel loaded Executable and Linkable Format (ELF) files. Its popularity among customers is undoubtedly due to it being a Linux kernel vulnerability. You can learn more about this CVE in the Red Hat CVE database, which also provides links to product-specific security advisories and other valuable resources.

CVE-2017-1000367 (Red Hat impact score: Important)

Days embargoed: **8**
Days from public notification to patch release: **0**
Total errata released: **2**

Made public on 2017-05-30, this vulnerability highlights the unique difference between an NVD rating of 6.4, and Red Hat Product Security's CVSS v3.0 scoring of 7.8. We determined the potential negative impact of exploitation from this vulnerability would be greater than that reflected by NVD scoring.

Although both NVD and Red Hat use the same CVSS v3.0 scoring calculator, our assessment of two characteristics varied, resulting in a much higher risk score. Specifically, we determined the "Attack Complexity" was Low, and the "Privileges Required" were also Low. These two values increased the overall vulnerability score. You can learn more about this CVE in the Red Hat CVE database, which also provides links to product-specific security advisories and other valuable resources. Additionally, customers reviewing this CVE should also review the related CVE-2017-1000368.

CVE-2017-6074 (Red Hat impact score: Important)

Days embargoed: **5**
Days from public notification to patch release: **0**
Total errata released: **15**

Made public on 2017-02-22, this kernel vulnerability (much like the other two kernel issues we described) gained quite a bit of interest from customers. For this vulnerability, it was determined the attacker would require local access. You can learn more about this CVE in the Red Hat CVE database, which also provides links to product-specific security advisories and other valuable resources.

NOTE: Customers can adjust the scoring of any CVE to align with their risk policies and environments. For example, see the score calculation for CVE-2017-6074. One of the more common changes made in the calculator is to change the "Attack Vector" to Network, which results in its highest value. This particular CVE is not exploitable over the network, but if it were, the calculator shows that it would not change the impact rating category—it remains Important.

CONCLUSION

While complete elimination of risk is impossible, reducing it to an acceptable level is achievable. At Red Hat we believe that security is a mindset, not a feature. That's why we work closely with upstream developers and communities to encourage secure coding practices, information sharing, and collaboration. We firmly believe the principles of open source software contribute to transparency and more secure products, benefiting customers and communities alike.

Even with strong security coding practices, community collaboration, and transparency, it is always possible for software vulnerabilities to exist. Red Hat strives to quickly respond to vulnerabilities that matter. In 2017, we saw a relatively small increase in the number of security errata issued and a relatively small decrease in flaws that were fixed, parallelled with a few products reaching their end of life.

Whether or not the vulnerability had a catchy name, we reviewed it. This resulted in almost 1,000 reported vulnerability impact assessments. We also considered the CVSS v3.0 score that was assigned to the vulnerability, but we did not allow it to be the sole factor when deciding what mattered. In some cases we evaluated flaws to be of a higher or lower impact, and prioritized our efforts accordingly.

Red Hat Product Security aims to exceed our customers' high expectations, and we implement a proactive approach to identify, assess, and address vulnerabilities. Each year we refine our approach and processes to respond swiftly to those vulnerabilities that impact our customers.

If you have vulnerability information you would like to share with us, please send an email to secalert@redhat.com. For inquiries or comments about this report, please reach out to our customer service team.

ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

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

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

redhat.com
F9726_0918