RED HAT PRODUCT SECURITY RISK REPORT: 2018

TABLE OF CONTENTS

INTRODUCTION

This report explores the state of security risk for Red Hat® products for 2018. We will describe our methodologies for working with security vulnerabilities, look at the performance data and metrics across our solutions, review the vulnerabilities that our subscribers and the larger industry were concerned about over the last year, and talk about how our products were affected by some of these issues.

When we refer to a product in this report, we mean a Red Hat offering listed at https://access.redhat.com/products. Our methodology included reviewing the vulnerabilities we addressed and the severity rating assigned to them by Red Hat, then looking at which issues were of meaningful risk and which issues were exploited. The data used to create this report is available from public data maintained by Red Hat Product Security, the team within Red Hat that works on (among other things) understanding and remediating flaws that affect Red Hat products. Red Hat Product Security assigns a Common Vulnerabilities and Exposures (CVE) name to every security issue we fix. If we fix a general bug that later turns out to have had a security implication, we go back and assign a CVE name to that issue. Every CVE fixed has an entry in our public database in the Red Hat Customer Portal, as well as a public bug report with more technical detail. In this report, we will use "vulnerabilities" and "CVEs" interchangeably.

Note: Red Hat uses a consistent methodology to allocate names and score severity so you can compare issues by Red Hat products or by dates. We do not recommend that you compare Red Hat product vulnerability count data (such as the number of CVEs addressed) to other companies' products, because assigning and reporting practices within organizations can vary considerably. Even among products from different Linux® vendors, the same CVE can have different effects, depending on how the product is built or integrated.

Across all Red Hat products, and for all issue severities, we fixed more than 1,270 vulnerabilities by releasing more than 745 security advisories in 2018

VULNERABILITIES

Across all Red Hat products, and for all issue severities, we fixed more than 1,270 vulnerabilities by releasing more than 745 security advisories in 2018. While that may sound like a large number, for context, the 2018 numbers resemble the number of vulnerabilities reviewed and assessed in 2017. All software programs are different and contain different bugs, so using a vulnerability count is not a fair measure of comparing one product to another. Assigning and reporting practices vary greatly (as we have cited previously) from industry to industry and product to product. If you look solely at Linux vendors, the same CVE can have different effects depending on how the product is compiled or deployed. Even within a single product like Red Hat Enterprise Linux, there is the potential for high variability. Red Hat Product Engineering crafts a default deployment configuration that system administrators have the flexibility to alter and either add to or disable features, but the product out of the box has a suggested set of configurations, and not every package is installed, nor are some even likely to be installed in an enterprise installation.

Red Hat uses a four-point scale to objectively describe the severity of a particular bug based on a rigorous analysis of the flaw. This scale was designed to align closely with similar scales used throughout the industry by other vendors or upstream open source communities. The severity levels are intended to help users determine which issues matter most. Ideally, this prioritized risk assessment helps customers understand how they are exposed and allows them to better schedule updates to the systems they manage. We recognize that each business is unique, with their own requirements and challenges, and that all risks are not created equal, nor are they the same company to company.

Red Hat Product Security uses the industry-standard Common Vulnerability Scoring System (CVSS) with each vulnerability we address. All CVEs impacting Red Hat products are issued a CVSSv3 score. CVSS is useful to describe how an attack works, however there are limitations in what it can describe, and therefore Red Hat does not use CVSS to prioritize vulnerabilities.

Our four-point scale rates vulnerabilities as Low, Moderate, Important, or Critical. Critical vulnerabilities pose the most severe risk to an organization. As described in our rating methodology, a Critical vulnerability could be exploited remotely over a network or the internet and could be automated by a worm. We expand this definition, like many of our peers, to also include flaws that affect web browsers or plug-ins that a user might be susceptible to if they visited malicious or compromised websites.

The table below compares the vulnerability counts of a subset of our Red Hat Enterprise Linux (RHEL) product family. A single Red Hat Security Advisory (RHSA) will often fix multiple vulnerabilities across multiple versions of a product. We view the vulnerability count as a general indication of the amount of effort a customer will spend to understand and fix the issue within their environment.

TABLE 1. RHSA COMPARISON CHART 2018

PRODUCT	CRITICAL ADVISORIES	IMPORTANT ADVISORIES	CRITICAL VULNERABILITIES	IMPORTANT VULNERABILITIES
All supported products	111	404	57	268
Red Hat Enterprise Linux 5,6,7 (combined)	29	132	22	140
Red Hat Enterprise Linux 7 (all packages)	16	97	21	136
Red Hat Enterprise Linux 5,6,7 (supplimentary packages)	30	42	26	111
Red Hat JBoss® Middleware	15	64	7	30
Red Hat OpenShift®	20	7	3	8
Red Hat OpenStack® Platform	0	16	0	5

In 2018, Red Hat addressed 1,272 total CVEs through 745 RHSAs across our entire portfolio. If we review these numbers closer, we will see that we issued 111 Critical security advisories that addressed 57 Critical CVEs. Of these Critical security advisories, 38% were issued within one day of the issue becoming public. Looking at the average delivery time for Critical advisories, you can see these were delivered within 18 days of the issue becoming public, with a median being 2.5 days. For issues rated as Important, 268 CVEs were addressed through 404 RHSAs during the same timeframe. For these vulnerabilities, 21% had patches available within one business day, with the average delivery time of 63 days and the median 8 days.

The year at a glance:

- 3,774 security issues were reported to Red Hat Product Security (nearly double the amount reported in 2015)
- 1,272 CVEs were addressed throughout 2018, an 11% increase from 2017
- 745 Red Hat Security Advisories were issued, a continued increase over previous years
- 111 Critical advisories addressing 57 Critical vulnerabilities
- 38% of Critical issues were addressed within 1 business day
- 80% of Critical issues were addressed within 1 week

To also put some of the numbers in context, many of Red Hat's products are layered on top of the solid foundation of RHEL. Those layered products are dependant upon a platform product like Red Hat Enterprise Linux to run. So while a product like Red Hat OpenStack Platform (OSP) or Red Hat OpenShift Container Platform (OCP) may have relatively less product-CVEs and RHSAs

during the calendar year (the OSP team directly dealt with 33 CVEs and 53 RHSAs total while our OCP team addressed 30 CVEs through 35 RHSAs), administrators of those platforms will need to also address many of the lower-level CVEs/RHSAs that are part of the underlying RHEL deployment.

These results highlight Red Hat's unique position up and down the stack. Red Hat is able to understand the nuances of systems installed using our portfolio of products and provide advice and insight on what the risks are in that combined solution. With practices honed over 25 years in creating and supporting Red Hat Linux and Red Hat Enterprise Linux, our newer offerings inherit all of those good practices and knowledge that helps Red Hat react quickly as flaws are discovered and reported.

Looking back to Table 1, the numbers reflect default installations of those products. Red Hat products are delivered in a generally secured state with reasonable, secure defaults (which are intended to cover the maximum amount of reasonable business use-cases) and services enabled. Customers looking to reduce their threat footprint should consider additional hardening beyond the defaults as detailed in documents like the Red Hat Enterprise Linux 7 security guide. The steps and techniques listed help further protect systems. Along with that guidance, customers can install or remove packages and processes they do not need to reduce the potential threats they might be exposed to throughout the normal course of operations.

VULNERABILITY TRENDS

As technology and organizations evolve, new business problems arise. As these problems become known, Red Hat will continue to use our experience to address the problems and create new solutions as needed. Red Hat is constantly changing and releasing new products to help meet these demands. With more products comes the potential for more vulnerabilities. In general, the number of vulnerabilities fixed annually continues to increase. When looking at a specific product, we tend to find fewer vulnerabilities over time as issues get addressed through our security backporting practices and fewer code changes, which could introduce new issues, are included.

We use the term backporting to describe the action of taking a fix for a security flaw out of the most recent version of an upstream software package and applying that fix to an older version of the package we distribute. Our backporting efforts help us deploy automated updates to customers with less risk.

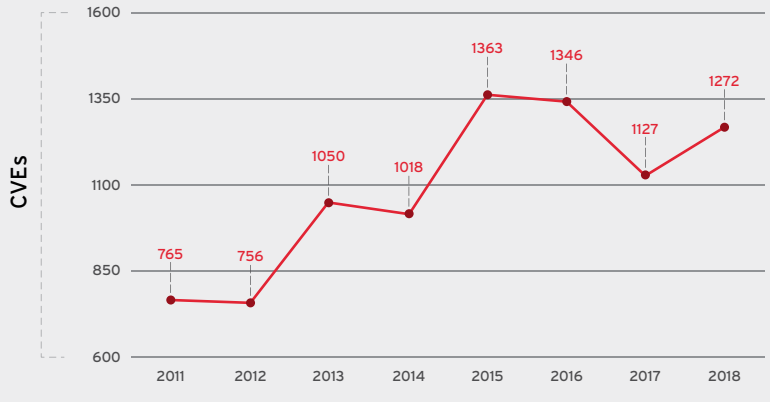

Figure 1. Red Hat security timeline

A vulnerability may get a catchy name, fancy logo, or media attention, but that does not mean that it poses a material risk to users.

For readers interested in exploring our data further, Red Hat Product Security offers several options. All of our security data is published publicly through multiple channels including the Red Hat Customer Portal security metrics page and our Red Hat security data application programming interface (API).

WHICH ISSUES WERE BRANDED, AND WHICH REALLY MATTERED, IN 2018

CVE-2014-0160 aka OpenSSL's Heartbleed vulnerability greatly impacted the security landscape for the technology industry. This instance was the first time a computer flaw was branded. This new naming practice drew substantial media and consumer interest, and even in 2018, branding of flaws became a common practice among security researchers.

Like the risks they could introduce, not all flaws are created equally, nor are they as severe as a flashy headline might suggest. Heartbleed and all the branded flaws that followed in its path have changed how vulnerabilities are now reported to vendors and open source projects. While it has raised the interest in cybersecurity and vulnerability response, history will tell us if the attention was justified as this trend continues.

As we have mentioned in previous reports, a vulnerability may get a catchy name, fancy logo, or media attention, but that does not mean that it poses a material risk to users. These words help guide Red Hat Product Security in how we react and inform the public on these highly publicized issues. To help best serve our customers and communities, Red Hat Product Security developed a process we term our customer security awareness program to help cut through the fear, uncertainty, and doubt that accompany many of these problems.

Through the customer security awareness program, Red Hat puts together a cross-organizational team to deal with issues that are either severe and could introduce high levels of risk to customers or threaten to generate a large amount of media attention that might distort the real risks and requirements to act. Red Hat delivers high-quality technical and remediation information as part of our vulnerability response articles. These articles include additional information above and beyond our standard security advisories, such as Red Hat Insights rules and detection scripts to understand the scope of where your systems might be exposed, Ansible® Playbooks that help detect and mitigate the vulnerabilities, and detailed descriptions of the underlying technical flaws and, whenever possible, if there are alternate mitigations available to work around them.

We believe that it is better to manage risks versus letting risks manage you.

Below are the highest-profile issues our products and the larger technology industry dealt with in 2018.

SPECTRE & MELTDOWN (January 3, 2018) CVE-2017-5753 CVE-2017-5715 CVE-2017-5754

Severity rating: IMPORTANT

2018 immediately greeted the world with three security issues collectively referred to as Spectre (CVE-2017-5753 & CVE-2017-5715) and Meltdown (CVE-2017-5754). These issues introduced the world to a new class of vulnerabilities related to flaws in microprocessors that affected most modern computers. Due to how CPUs have been optimized for performance, a local attacker could potentially read data in memory that they were not authorized to read.

We believe that it is better to manage risks versus letting risks manage you.

These issues affected supported versions of Red Hat Enterprise Linux, Red Hat OpenStack Platform, Red Hat Virtualization, Red Hat Enterprise Linux Atomic Host, and Red Hat Enterprise MRG. They required both software (kernel/virtualization) and hardware (microcode/firmware) fixes to mitigate the exploit. Patches for current release streams were available starting the same day the flaws went public, with older products receiving patches over the next several days. The initial mitigations were revised and performance was improved with the release of retpolines starting in March 2018. The content created in response to this issue and those that followed were some of the most viewed on our Customer Portal for the year with over 180,000 views on the vulnerability article alone. This also started our Vulnerability explained in 3 minutes video series which was widely cited throughout the industry. There are no known working public exploits for any of these issues to date.

Source-to-Image Vulnerability -S2I (April 27, 2018) CVE-2018-1102

Severity rating: CRITICAL

A bug was discovered in the Source-to-Image build functionality used within Red Hat OpenShift Container Platform that could allow an unprivileged user to escalate their privileges and gain access to the host system in the cluster. This issue affected all 3.x versions of Red Hat OpenShift Container Platform supported at the time. This was the first major issue coordinated with the upstream OpenShift community.

Red Hat had patches available for impacted versions of OpenShift Container Platform starting within one business day, with work-around mitigations available at the time the issue was made public.

POP SS debug exception (May 8, 2018) CVE-2018-8897 & CVE-2018-1087

Severity rating: MODERATE & IMPORTANT

Two related issues (one for bare-metal systems and the other focused on virtualized systems) that revolved around a flaw in how stack-switch operations were handled in MOV to SS or POP SS instructions. On bare-metal systems, this flaw could lead to a denial of service attack and impact a system's availability. In a virtualized system, an unprivileged KVM guest user could use this flaw to crash the guest or, potentially, escalate their privileges in the guest. With the scope of the virtual machine attack being broader, the CVE was rated IMPORTANT, rather than MODERATE.

These issues affected all currently supported versions of Red Hat Enterprise Linux, Red Hat Enterprise Linux Atomic Host, Red Hat Enterprise MRG, and Red Hat Virtualization. Patches were available for all impacted products within one business day of the issue being made public.

DHCP Client Script Code Execution Vulnerability (May 15, 2018) CVE-2018-1111

Severity Rating: CRITICAL

A provided script to configure DHCP client packages (dhclient) could lead to a command injection attack in Red Hat Enterprise Linux 6 and 7 and Red Hat Virtualization 4. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses, could use this flaw to execute arbitrary commands with root privileges on systems using NetworkManager, which by default is configured to obtain network configuration using the DHCP protocol.

Patches and mitigations were made available the same day the issue was made public.

Kernel Side-Channel Attack using Speculative Store Bypass (May 21, 2018) CVE-2018-3639

Severity rating: IMPORTANT

With this microprocessor flaw, an unprivileged attacker could bypass restrictions to gain read access to privileged memory that would otherwise be inaccessible. This issue was also referred to as Variant 4 or Speculative Store Bypass. This issue is known to affect CPUs of various microarchitectures. All supported versions of Red Hat Enterprise Linux, Red Hat OpenShift, Red Hat Virtualization, and Red Hat OpenStack Platform were affected.

A malicious, unprivileged user could use this flaw to read privileged system memory and memory outside of a sandboxed environment like a web browser or JIT execution run times.

Patches for this issue were available starting the day the issue was made public and continued to be released for a month afterwards. To fully mitigate this vulnerability, system administrators had to apply both hardware microcode updates and software patches that enabled new functionality.

L1TF - L1 Terminal Fault Attack (August 14, 2018) CVE-2018-3620 & CVE-2018-3646

Severity rating: IMPORTANT

Similar to Spectre and Meltdown, these vulnerabilities could allow an unprivileged attacker to bypass memory security restrictions to gain access to data stored in L1 cache that would otherwise be inaccessible. Also referred to as Foreshadow, these issues are known to only affect x86 microprocessors manufactured by Intel at this time. Both flaws require software-level mitigations performed by operating systems and hypervisors. Full mitigation from potential attack by untrusted guest virtual machines in an environment using virtualization will require specific action by a system administrator including disabling simultaneous multithreading (SMT), also known as hyper-threading (HT).

This issue affected supported versions of Red Hat Enterprise Linux, Red Hat OpenStack Platform, Red Hat Virtualization, Red Hat Enterprise Linux Atomic Host, and Red Hat Enterprise MRG. Patches for this issue were available starting the day the issue was public and continued to be released for the next two weeks.

In virtualized, cloud, or container environments, additional risk analysis is needed to understand how workloads are managed within the environment. Co-mingling of known, trusted workloads alongside untrusted or lower security instances potentially exposes other guests and control infrastructure to a malicious actor reading data stored within L1 cache of the host system's CPUs. Ultimately, barring workload isolation, the only way to ensure that the risk for this particular attack was mitigated would be to disable hyper-threading, which is not an inconsequential decision for most organizations.

Kubernetes privilege escalation (December 2, 2018) CVE-2018-1002105

Severity rating: CRITICAL

A flaw in Kubernetes, a container orchestration platform used in Red Hat OpenShift releases, was discovered that could allow a malicious actor to escalate their privileges and compromise other pods within a Red Hat OpenShift cluster. A second flaw that could allow a malicious party to escalate their permissions and gain cluster-wide administrative-level permissions through an aggregated API server was also revealed at the same time.

All supported versions of Red Hat OpenShift were affected, including Online and Dedicated. Patches for this issue were available starting the day the issue was public, and all supported versions had fixes available within 24 hours of public disclosure.

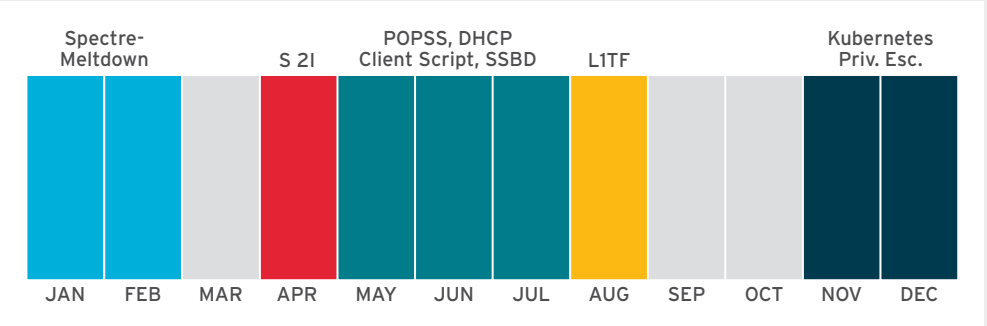

Figure 2. A tour of the most significant vulnerabilities in 2018

LEGEND

Issues denoted in red were branded flaws. Issues denoted with a computer chip were related to microprocessor issues

1. Spectre and Meltdown
   CVE-2017-5715
   CVE-2017-5753
   CVE-2017-5754
2. SSBD
   CVE-2018-3639
3. L1TF/Foreshadow
   CVE-2018-3620
   CVE-2018-3634
4. SegmentSmack
   CVE-2018-5390
5. dhcp command injection
   CVE-2018-1111
6. kubernetes authentication bypass
   CVE-2018-1002105
7. POP SS
   CVE-2018-1087
   CVE-2018-8897
8. libssh authentication bypass
   CVE-2018-10933
9. SSL/TLS Birthday attack (Sweet32)
   CVE-2016-2183
10. Fragmentsmack
    CVE-2018-5391

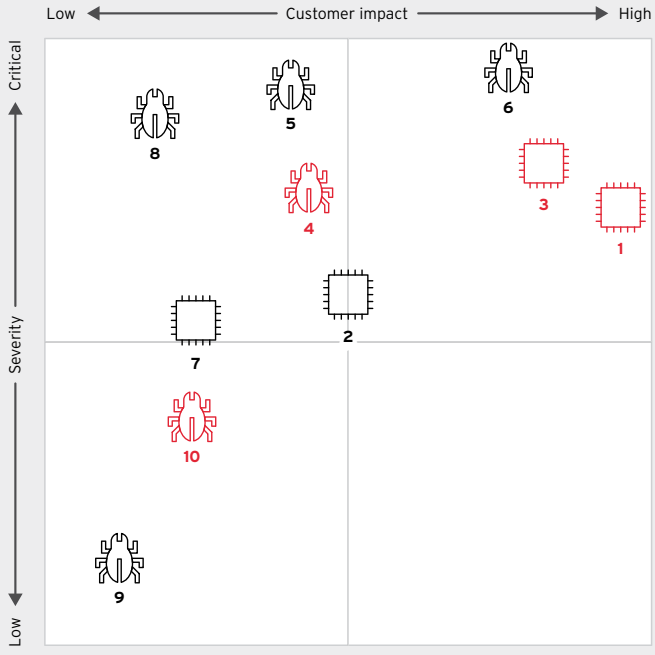

Figure 3. Lower risk issues with increased customer attention

In Figure 3 above, we have plotted what we deemed the 10 most interesting vulnerabilities based off of two data factors: the severity of the CVE(s) and the impact to our customers. Each customer is unique, so they may not use a particular package, or they may have other controls in their environment that decrease the residual risk of a given flaw. Conversely, a system affected by any of the 1,274 vulnerabilities addressed in 2018 could support business-critical systems or have other factors that increase the risk for the affected organization.

Another way we gauge customer interest is to measure web traffic, specifically, views for each CVE page in the Red Hat Customer Portal.

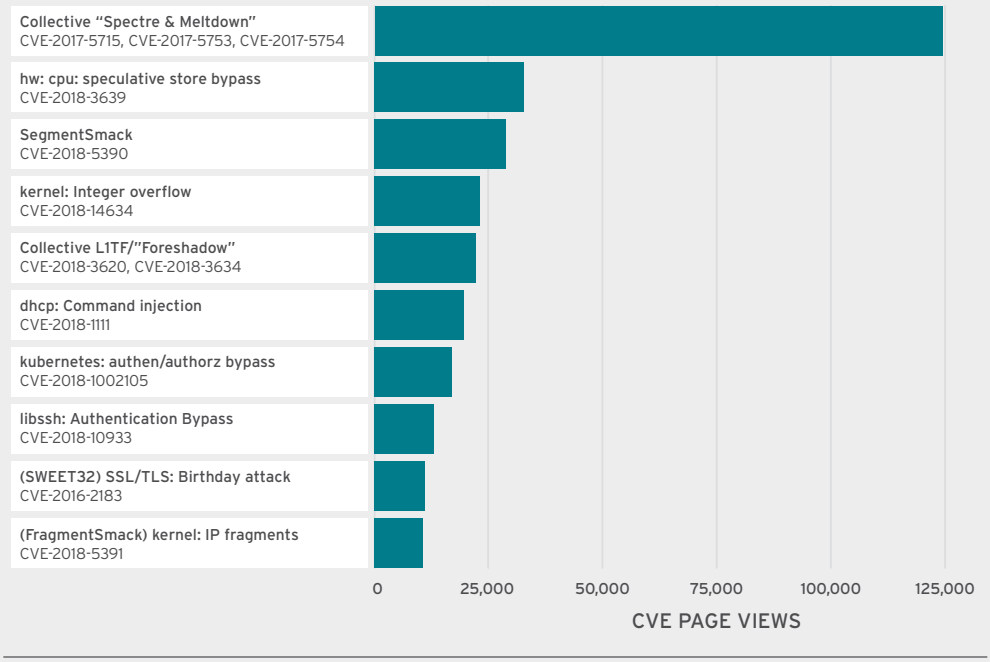

Figure 4. Gauging customer concern

The issues detailed in Figure 4 were the most-viewed vulnerabilities from the Red Hat CVE database. Customer interest in Spectre and Meltdown occupied a significant amount of attention over the year, bringing in nearly four times the page views of the next most visited CVE page, SSBD.

THE OPEN SOURCE SUPPLY CHAIN

All Red Hat products are based upon and heavily contribute back to open source communities and projects. A given Red Hat product could contain thousands of individual packages, many based upon a separate third-party package from an open source upstream. Red Hat engineering participates in developing and maintaining many of these upstream components that are the vital foundation of innovation for our enterprise product offerings. Managing and tracking vulnerabilities across these thousands of third-party components is a significant effort, which is why Red Hat has a dedicated Product Security team that monitors issues affecting Red Hat products and the projects and packages that comprise them. The Product Security team also works with our industry peers and security researchers. As vulnerabilities are discovered, Product Security works with Product Engineering and upstream communities to ensure that the issues are documented and prioritized to deliver fixes as quickly as possible to our subscribers—and to the open source community at large.

In 2018, we investigated over 3,774 vulnerabilities that potentially affected parts of our products. These efforts led to the confirmation of impact and resolution of 1,274 of those reported. Each one of those 3,774+ vulnerabilities is tracked within the Red Hat Bugzilla tool and is publicly accessible. Each vulnerability has a master bug, including the CVE name as an alias and metadata such as the dates we discovered it or were notified about it, its severity, and its source. Issues that are not yet public (which are referred to as embargoed) still get an entry in bugzilla, although during the embargo period they are kept private and shared only with those engineers and contributors that need to know about them and can help collaborate on fixing them. As the flaw gets disclosed to the public, the associated bugzilla is updated and also made public. This data is all available through multiple streams for anyone to review:

- Metrics webpage
- Red Hat Security Vulnerability Data API
- OVAL and CVRF data feeds
- RHSA announcements

We use this data to create metrics and review trends with product engineering to help improve future releases and the whole open source ecosystem.

Red Hat does not wait for the bugs to come to us. Our Engineering, Quality Assurance, and Security teams are all actively looking for and finding issues. Approximately 29% of the issues Red Hat addressed came to us directly from peers or Red Hat employees. This is slightly down from 2017, but the number of total flaws reported grew 11% over the previous year. When possible, we share these issues back upstream and with our industry peers. In addition to those issues, Red Hat may also find and report software flaws that are not part of our currently shipped products. When it comes to fixing issues in third-party software, relationships matter. Red Hat Product Security and Product Engineering have deep ties to upstream communities and the technology industry at large. We are constantly communicating and collaborating with our peers on issues that impact all of our shared customers and communities.

If an upstream community is willing to share information about flaws with us in advance, we feel a responsibility to give value back for that shared trust. We do this by reviewing advisories, checking patches, and feeding data back from our quality or performance testing groups. Ultimately we're all focused on providing remediation to the flaws, and we all try to contribute positively to the solution as it is evolving.

CONCLUSION

We hope that this report has provided useful information about the risks and flaws addressed across the Red Hat portfolio in 2018. Looking at the flaws reported and fixed over the years, we can see that, in general, the number of vulnerabilities found and fixed continues to rise over time.

There are other types of risks that enterprise operations has to deal with that we do not address in this report, specifically, malware or ransomware. These types of attacks typically rely upon the attacker having or gaining access to a system through intrusion or exploiting a person or vulnerability. Social engineering relies upon the innate good-nature of humans, and sometimes due to the existence of some level of permission or technical flaw, the persuasive attacker can exploit their target. Effective risk management practices, like a rigorous and speedy patch management process, measured and audited access controls, and logging, all help reduce the likelihood of a successful attack, and the overall impact if a flaw does gets exploited.

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 integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

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
F16049_0219