Juniper Networks | Driven by Experience™

A Day in the Life of a Security Vulnerability

The Juniper Security Incident Response Team (SIRT) tracks security vulnerabilities from discovery to remediation

White Paper

Table of Contents

Executive Summary 3
Introduction 3
Juniper SIRT History 4
Breadth of SIRT Coverage across Juniper Products 4
Tracking Through End of Engineering 5
The Advent of Product Security Incident Response Teams 5
SIRT Composition and Roles 6
Incident Managers 6
Product Security Engineers 6
Street Cred—Industry Influence and Leadership 7
Forum of Incident Response and Security Teams Member and Active Participant . 7
Industry Consortium for Advancement of Security on the Internet 7
Fixing Software Releases 8
How Juniper Prioritizes Security Bug Repairs 8
Juniper Security Advisories 8
What Is a JSA? 8
Drafting Security Advisories 9
How Many JSAs Are in a JSA Bundle Each Quarter? 9
In-Cycle, Quarterly Advisories 9
The JSA Cycle 9
The Quarterly (90-day) Cycle Highlights 10
Handling Security Flaws Found Near Quarter End 11
JSA Bundle Publication 11
Out-of-Cycle Advisories 11
Conclusion 12
About Juniper Networks 12

Executive Summary

Today, enterprise organizations are increasingly aware of the cost of data breaches. According to a recent IBM report,[1] the global average total cost of a data breach was nearly $4.5M. In the U.S., the average cost of a data breach was much higher—twice the global average, in fact. Without considering the detrimental effects of a security breach on an organization's credibility and trustworthiness, recovering from a successful cybercriminal attack is not inexpensive.

While everyone should be aware of the high costs of breaches and how to prevent them, this white paper isn't about data breaches or the malicious threat actors perpetrating such attacks on enterprises and government organizations. Not exactly. Instead, the focus of this paper is on managing the product security vulnerabilities that—if not remediated—lead to exploitation and subsequent data breaches.

More specifically, the paper is about the groundbreaking Juniper® Security Incident Response Team (SIRT) that is responsible for product security incident management at Juniper. This paper tells the SIRT story. It explains SIRT's industry-leading processes and procedures—methods that Juniper SIRT, in one form or another, has been following to protect Juniper customers for more than 20 years.

Introduction

Few would argue that software—no matter the product, no matter the developer—has flaws in it. And while some flaws, or bugs, may have to do with functionality or cosmetics, what's important is whether the bug can be triggered by an attacker to do something bad. These kinds of shortcomings are security vulnerabilities, and if exploited, they can lead to data breaches and/or denials of service. Therefore, it is incumbent upon computer and networking companies to stand ready to find and remediate security-related bugs before cybercriminals and other malicious threat actors exploit them.

Juniper has always taken a proactive approach to improving and securing its products while being transparent about it. By being transparent, Juniper builds trust with its customers and the security community. SIRT is the reflection of Juniper's commitment to security and transparency. Working in collaboration with groups inside and outside of Juniper, SIRT's mission is to track all security vulnerabilities in Juniper's hardware, software, and firmware from discovery to remediation.[2]

[1] www.ibm.com/downloads/cas/3R8N1DZJ
[2] Over the years, about 95% of the vulnerabilities that have been uncovered and remediated are in software.

Juniper SIRT History

Following the Morris worm outbreak that crippled the then young Internet (see “The Advent of Product Security Incident Response Teams”) and during the last decade of the 20th century, technology companies realized they had a security problem. The Computer Emergency Response Team Coordination Center (CERT/CC) in the U.S. rose to the occasion and launched an effort to simplify and improve communication with computer, networking, and network security equipment makers. CERT/CC appealed to these product manufacturers to allocate a single resource inside their respective companies to facilitate security vulnerability communication.

In response to the call, Juniper appointed a principal technical support engineer to be its point-of-contact (PoC) to CERT/CC. Other computer and network product manufacturers, including a company called Unisphere Networks, followed suit. In 2002, Juniper acquired Unisphere. Following the acquisition, the individuals at Juniper and Unisphere who had been CERT/CC PoCs discussed the way forward for Juniper in terms of security incident handling. The trail they blazed led to the birth of Juniper SIRT.

Though the official name, “Juniper SIRT,” wasn’t adopted until 2004, Juniper has been following its industry-standard, product-security, incident response-related processes and procedures for more than two decades—almost all the way back to our founding in 1996 and prior to the Morris worm outbreak.

Breadth of SIRT Coverage across Juniper Products

Juniper SIRT's domain extends across all Juniper product lines. Thus, the breadth of SIRT coverage includes Juniper's core, legacy product lines and products under the Juniper umbrella that resulted from acquisitions.

Even so, Juniper has historically developed and manufactured routers, switches, and firewall products. It's unsurprising, then, that the lion's share of security vulnerabilities, tracked by Juniper SIRT from discovery through remediation, were found in the two Juniper operating systems, Junos® OS and Junos OS Evolved, that run on these kinds of systems.

Tracking and managing security vulnerabilities on these operating systems is no easy feat. That’s, in part, because between the Junos OS and Junos OS Evolved operating systems alone, many major versions are supported at any one time. Counting maintenance and support releases, still more versions of these two operating systems are actively supported by Juniper and monitored by SIRT. So, if you guessed that SIRT is busy with much to track, you have guessed right!

Tracking Through End of Engineering

For practical reasons, security incident response personnel at any computer and network equipment manufacturer must determine the point at which their organization will stop tracking, confirming, and working (with internal teams, typically) to resolve security vulnerabilities in a product. For Juniper SIRT, that point arrives when the product is at the End of Engineering (EOE) product life-cycle stage.

Once a Juniper product reaches EOE, six additional months typically remain (for many Juniper products) until the product reaches end of support (EOS) in the Juniper product life cycle.

Service tickets may still be opened and closed between EOE and EOS. What is important for Juniper customers to be aware of is that SIRT does not track, does not confirm through testing, and does not produce Juniper Security Advisories (JSAs)—more on those later—for any security vulnerabilities found after EOE in the product life cycle.

The Advent of Product Security Incident Response Teams

In November 1988, the Morris worm, a self-replicating computer worm that exploited several vulnerabilities in systems running BSD Unix, gained national attention for wreaking havoc on the then young, worldwide network of computer systems, known as the Internet. There was no coordinated response to the worm attack. Instead, there was a duplication of effort, wasted resources, and conflicting solutions.

Following this debilitating, Internet-impacting, denial-of-service (DoS) attack and in recognition of the need for a central organization to coordinate responses to similar network emergencies, the Defense Advanced Research Projects Agency (DARPA) in the U.S. funded the establishment of the Computer Emergency Response Team Coordination Center (CERT/CC).

Around that time, computer, networking, and network security product manufacturers began to recognize, if they hadn't already, that their products may one day be susceptible to exploitation following a similar "security incident." That meant that they too would have to track, prioritize, and remediate security vulnerabilities in their own products.

Acting on these realizations, companies like Juniper began conceiving and shaping product security incident response teams (PSIRTs). After all, Juniper was developing and continues to manufacture the routers, switches, and firewalls that pass and protect information in transit across the Internet.

SIRT Composition and Roles

Juniper SIRT is comprised of two groups: Incident Managers (IMs) and Product Security Engineers (PSEs).

Incident Managers

The group of SIRT IMs has a singular goal, which is to shepherd security bugs from discovery to remediation during that same calendar quarter in which the bug is resolved. The way in which IMs get assigned to track a particular security bug is as follows. Each week Juniper SIRT rotates a different SIRT IM from the group into the proverbial "hot seat." During that week, the IM in the hot seat takes ownership of any newly uncovered, security vulnerability problem reports (PRs) identified in GNATS, the system Juniper uses to track bugs.

Over the course of time, each SIRT IM becomes responsible for an approximately equal number of product security vulnerabilities. Once they are tracking a particular security vulnerability, one of the first tasks the IM performs is he or she calculates the industry-standard Common Vulnerability Scoring System (CVSS) base score for the security vulnerability.

For security vulnerabilities tracked by an IM that have a higher CVSS score and that have been fully remediated during a particular calendar quarter, the IM produces a JSA. As all IMs are working on JSAs, someone in the IM subset of SIRT has to be responsible for publishing the set of JSAs. Therefore, SIRT quarterly rotates a different IM in to be the JSA "bundle commander." He or she manages the 90-day countdown (more on that later) leading to the creation and publication of a new, in-cycle JSA bundle.

Product Security Engineers

Juniper SIRT PSEs, on the other hand, work in a lab environment, replicating whenever possible all discovered security vulnerabilities on a representative sampling of impacted platforms.

Similarly, once the Juniper engineering team fixes any shortcomings, SIRT PSEs demonstrate through additional testing that the fixes do indeed repair the affected product(s). In doing so, SIRT PSEs strive to test fixes for a given vulnerability on a sampling of affected platforms (if more than one platform was impacted).

SIRT PSEs, because of the testing they perform, gain an intimate understanding of any security shortcomings. This mastery and deep grasp of the security bugs gained by PSEs through testing raises the performance level and overall quality of the work performed by Juniper SIRT. SIRT PSEs document potential workarounds, when they exist, and can describe the conditions that must be present for a vulnerability to be exploited—such as specific configurations as is often the case. Sharing this information with customers and internal teams is an invaluable service provided by Juniper SIRT and an example of how Juniper is raising the bar on customer expectations. Together, SIRT and Juniper work continuously to improve customer experiences.

Additionally, the resulting written and published Juniper JSA explanations are much more accurate and robust because PSEs have replicated security vulnerabilities and confirmed the fixes through testing.

Street Cred—Industry Influence and Leadership

Forum of Incident Response and Security Teams Member and Active Participant

To respond to international cybersecurity incidents, fight cybercrime, and improve the state of cyber defenses, Juniper SIRT engages with external, like-minded organizations such as the Forum of Incident Response and Security Teams (FIRST).[3] Comprised of nearly 700 "teams" distributed around the world in more than 100 countries (at the time of writing), FIRST teams range from National Computer Security Incident Response Teams (National CSIRTs) to Product SIRTs (like Juniper SIRT) to worldwide telecommunications providers to InfoSec incident response teams.

For nearly two decades (since 2006), Juniper has been a member of FIRST and actively engaging with member organizations, often in a leadership capacity. In fact, the director of Juniper's SIRT twice served on the FIRST board of directors. In total, he served a combined 12 years on the FIRST board, longer than any previous board member. Also, over the years, Juniper SIRT leaders chaired—and continue to chair— various FIRST special interest groups (SIGs) including one that is developing the next generation of the CVSS. This SIG is responsible for evolving CVSS from version 3.1 to 4.0. Their aim is to dramatically expand the applicability of CVSS to everything on the network, including Internet of Things (IoT) devices, industrial control systems (ICS), operational technology (OT), and beyond.

In addition to all that, Juniper SIRT leaders are on the FIRST program committee that selects content, after assisting with the review of proposed submissions, for FIRST's multistakeholder forums and conferences.

Industry Consortium for Advancement of Security on the Internet

In 2008, the Industry Consortium for Advancement of Security on the Internet (ICASI) was launched, "to strengthen the global security landscape by driving excellence and innovation in security response practices; facilitating collaboration among members to analyze, mitigate, and resolve multistakeholder, global security challenges."[4]

When founded, ICSAI was a trust-based organization comprised of five companies: Cisco, IBM, Intel, Microsoft, and Juniper. Using ICASI's unique, multiparty nondisclosure agreements, Juniper and these other companies—all of which were way ahead of the curve in terms of handling vulnerabilities and security incident response management—began sharing best practices and exchanging otherwise-private information.

[3] https://www.first.org/
[4] https://www.first.org/newsroom/releases/20210601

In 2021, ICASI was integrated into FIRST. Juniper SIRT subsequently helped facilitate and advise on the integration of ICASI into FIRST's PSIRT SIG, a merger designed to further help standardize and consolidate industry best practices.

Fixing Software Releases

How Juniper Prioritizes Security Bug Repairs

While Juniper fixes all security vulnerabilities as quickly as possible, Juniper uses CVSS scoring to prioritize the security vulnerabilities to be resolved and the scope of the resulting fixes into the Juniper code bases (Table 1).

Table 1: CVSS Score Determines Scope and Priority of Security Bug Fixes

CVSS Score	Scope and Priority of Security Bug Fixes
CVSS score < 3.0	Juniper fixes the security bug in the current, mainline release. Rather than fixing every currently supported release, incorporating the fixes into the current, mainline release ensures the security shortcoming is repaired going forward.
CVSS scores ≥ 3.0 but < 5.0	Juniper will fix the security bug in all supported releases.
CVSS score ≥ 5.0	Juniper takes these security vulnerabilities very seriously. In fact, security bugs with CVSS scores greater than or equal to 5.0 are considered a "blocker," meaning that the fix for the shortcoming needs to be incorporated into the immediately following Juniper code revision. For such security vulnerabilities, in addition to fixing the security bug in all supported releases and incorporating it into the immediately following Juniper code revision, SIRT IMs quarterly author and publish Juniper Security Advisories (JSAs) describing these vulnerabilities. SIRT does so only after Juniper development engineers prepare and incorporate working fixes into all impacted code releases.

Juniper Security Advisories

What Is a JSA?

A Juniper Security Advisory (JSA) is a written description documenting a security vulnerability in a Juniper product or products. SIRT produces JSAs primarily for Juniper customers. The JSA provides information and actionable intelligence for customers about the security bug in question. As explained in Table 1, SIRT IMs write and quarterly publish a JSA for fixed security vulnerabilities having a CVSS score greater than or equal to 5.0.

In terms of JSAs and CVE IDs,[5] there is either a 1:1 or 1:Many relationship. Most often there is a 1:1 mapping of a single JSA to one unique CVE ID. Even so, JSAs frequently contain more than a single CVE ID. For example, multiple open-source software components may have been updated with fixes having dozens of associated CVE IDs. In cases like this, a JSA may refer to more than a single CVE ID.

[5] Created by MITRE Corporation in 1999, Common Vulnerabilities and Exposures (CVE) IDs are commonly used by the security industry to catalog and describe security vulnerabilities in public-facing software. Thus, it is no surprise that a security vulnerability found in Juniper code typically has an associated CVE ID.

Drafting Security Advisories

Juniper SIRT walks a fine line when writing JSAs. On the one hand, SIRT recognizes that it must provide actionable intelligence to customers and internal account and support teams. On the other hand, SIRT must be judicious and careful not to provide any more information than is necessary to would-be attackers.

It's important to note that prior to in-cycle, quarterly JSA bundle publication—fixes and/or workarounds exist for each JSA. Because Juniper is careful in how it presents JSA content, and as there are fixes or workarounds available for customers to mitigate the threats, malicious threat actors gain no advantage. Customers remain protected.

How Many JSAs Are in a JSA Bundle Each Quarter?

On average, Juniper SIRT publishes 35 to 40 JSAs per quarter in a JSA Bundle. Some would argue that's too many security vulnerabilities. Competitors may feel compelled to use the quantity of flaws found as leverage to attack Juniper.

But here is the rub: Not all competitors publish the vulnerabilities they find internally. Other competitors may not even be looking for vulnerabilities! As for Juniper, roughly half of the uncovered security vulnerabilities that merit a security advisory are found internally by Juniper.

Juniper has always taken a different approach—a proactive and transparent approach—to improving and securing its products. By being transparent, Juniper builds trust with our customers and prospects.

Some have said, and Juniper agrees, that finding vulnerabilities and resolving them is actually an indicator of a mature process, rather than the other way around.[6] In other words, anything short of regularly searching out security vulnerabilities in your own products—and eliminating them—should raise an eyebrow and prompt questions from prospective buyers as well as existing customers.

In-Cycle, Quarterly Advisories

The JSA Cycle

Most often Juniper publishes the JSAs quarterly in a bundle (assuming there is more than one JSA to publish). As JSA Bundle publication has a regular, recurring rhythm, Juniper refers to it as being "in-cycle." The benefit of publishing with a regular cadence is that all Juniper stakeholders—from customers to internal account teams to support/service personnel—anticipate the publication, schedule available resources, and begin to determine how they're impacted, if at all.

[6] https://becomingahacker.org/increased-cve-counts-a-positive-indicator-of-a-maturing-security-ecosystem-126e18ea8d90

The Quarterly (90-day) Cycle Highlights

SIRT follows a set of processes and procedures to ensure consistency each quarter leading up to the publication of JSAs for higher severity vulnerabilities in Juniper products as outlined in Table 2.

Table 2: 90-day Countdown to Quarterly JSA Bundle Publication

Timeframe	JSA Activity
T minus 90 days (i.e., T-90)	The newly appointed JSA bundle commander performs administrative tasks to ensure SIRT begins the new quarter with a blank slate.
T-45	By this point in the quarterly cycle, Juniper SIRT has visibility into and certainty about the set of problem reports (PRs) from the GNATS defect tracking system, with CVSS scores >= 5.0, that are likely to be in the upcoming JSA Bundle for the quarter. Aware of that, the IM bundle commander sends this list of PRs to Juniper Release Management (JRM) alerting them that SIRT intends to publish JSAs corresponding to each of these PRs at quarter end. The JRM team, separate from SIRT, then works with relevant stakeholders in Juniper to ensure those PRs are indeed fixed and that the fixes are incorporated into all impacted releases.
T-44 through T-35	Individual IMs prudently draft JSAs for each security vulnerability they shepherd through the process from discovery to remediation. SIRT IMs write JSAs with a keen awareness that they must balance the need to explain the vulnerability to defenders while being mindful not to inadvertently provide excess information to would-be attackers bent on exploiting and attacking weaknesses in Juniper products for nefarious purposes. In drafting JSAs, SIRT is meticulous about using clear, precise language. In addition to being conscientious and wary about providing too much information for attackers, another SIRT objective in drafting these advisories is to ensure a consistent look and feel from one SIRT-written JSA to the next, regardless of which SIRT IM team member drafted the security advisory.
T-32 through T-20	Juniper SIRT hosts daily, internal meetings during this period to carefully review each security advisory drafted by the IM team.
T-15	Juniper SIRT IMs send their draft JSAs to the engineer(s) that fixed the corresponding security bug, inquiring as to whether the IM properly characterized the vulnerability.
T-6	Juniper SIRT conducts an internal briefing for all interested internal stakeholders including Juniper's service, support, and account teams. SIRT announces to those in attendance the set of JSAs in the soon-to-be-published bundle, summarizing the ones most likely to be of interest to customers. Following the SIRT briefing, account teams have the remaining 6 days to prepare such that at T-0 the account team is in a position to discuss, with customers interested in this service, the details of relevant fixed vulnerabilities.
T-0	The SIRT IM, acting as bundle commander for the quarter, publishes the JSA Bundle (more details about publication fare in “JSA Bundle Publication”).

Handling Security Flaws Found Near Quarter End

Sometimes a security flaw is discovered close to the end of Juniper SIRT's quarterly JSA release cycle. As a result, there may be too little time to replicate and/or to develop fixes for the vulnerability, let alone incorporate the fixes into and across all supported and impacted releases. In such cases, the security vulnerability does not make it into the current quarter's JSA Bundle and instead becomes part of the following quarter's Bundle.

JSA Bundle Publication

The JSA Bundle is published quarterly on the second Wednesday during the months of January, April, July, and October at 9am Pacific Time. On those dates, at that time, the IM who is the acting Juniper SIRT bundle commander publishes the previous quarter's JSA Bundle at https://advisory.juniper.net.

At that URL are listed each of the individual security advisories comprising the JSA Bundle, each having its own URL. Not just the current, but all previous JSAs are cataloged there as well. JSAs can be searched by product/series, by category of product, by operating system, and by severity.

In addition to updating the JSA repository on the Juniper website, customers that have subscribed to advisories receive an email indicating that the quarterly JSA Bundle has been published. Juniper SIRT also announces the news on its social media properties, including Twitter.[7]

Following JSA Bundle publication, as a CVE Numbering Authority (CNA), Juniper provides the National Vulnerability Database (NVD)[8]—among others—the complete list of new CVE IDs published during the recently-ended JSA quarterly cycle via the CVE Services API. As Juniper SIRT must occasionally make modifications (typically minor) to one or more recently published JSAs, SIRT waits a few days after the quarterly JSA Bundle is published before publishing the new CVE IDs.

Out-of-Cycle Advisories

Not all JSAs are published during the regular, quarterly cycle. On occasion, Juniper may need to publish an out-of-cycle JSA. For example, suppose a security vulnerability is being actively exploited. In that case, even if patches are not yet available, SIRT alerts and advises customers via an out-of-cycle JSA, explaining to them everything SIRT knows about the shortcoming. Thereafter, SIRT updates customers, as needed, until the issue is resolved with an effective, validated fix or workaround. Note too that for out-of-cycle advisories, in situations like the one described, Juniper SIRT typically provides some sort of mitigation to protect customers in the near term until a fix or workaround is available.

[7] Follow Juniper SIRT on X (formerly Twitter) @JuniperSIRT

[8] The U.S. Government, under the management of the National Institute of Standards and Technology (NIST) Computer Security Division, tracks known software security vulnerabilities by CVE ID in a database repository called the National Vulnerability Database (NVD).

Conclusion

Juniper customers can rest assured that Juniper products are continually being improved. Thanks to the efforts of an industry-recognized Security Incident Response Team that is second to none, Juniper has been following a mature set of product security incident response handling processes while quarterly shepherding security vulnerabilities from discovery to resolution. A visible sign of the culmination of successful security vulnerability remediation, Juniper SIRT quarterly publishes JSAs that provide actionable intelligence for its customers. For more than two decades, the work of Juniper SIRT is demonstrable evidence of Juniper's commitment to security, to continuous product improvement, and to building trust through transparency with its customers and prospects alike.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

JUNIPER NETWORKS | Driven by Experience™

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000 | Fax: +1.408.745.2100
www.juniper.net

2000812-001-EN Sept 2023