BGP Security Vulnerabilities and CVSS

Jeffrey Haas, Juniper BGP DE
Matt Paulsen, Juniper SIRT Sr. SecEng

Abstract

BGP's deployment model makes even modest software bugs to have a significant consequences on global Internet routing.

When is a bug just a bug and not a security issue?

CVSS is a scoring system used to assess the *severity* of security vulnerability issues and is an important input toward vendors issuing security alerts – and subsequently locking down all information on that issue.

We discuss BGP and CVSS severity scoring and its impact upon the availability of information on BGP implementation defects.

About CVSS

Common Vulnerability Scoring System (CVSS)

- https://www.first.org/cvss
- “The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its **severity**. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.”

Severity vs. Risk

- The CVSS Base score, provided by vendors, is not a scoring of *risk*, only *technical severity*.
- There's a strong desire to want to infer the risk of malicious exploitation from the CVSS Base score alone, but that was never the design goal.
- We see the industry at large using the CVSS Base score for risk assessment by itself *without further assessment*.
  - The CVSS Base score is a poor indicator for determining general risk.
  - Risk is situational!

Severity vs. Risk (2)

- CVSS Base score *should be* and generally *is not* expanded into Threat and Environmental assessment (CVSS-BTE) by the consumer
- Once we decide that the *severity* of the issue is high enough to issue a security advisory, we no longer discuss the details where those details may help an attacker more than the defender.
  - Lack of details makes gauging situational risk difficult to impossible!

What Juniper (and the industry) uses CVSS for

- CVSS v4.0 was released on November 1, 2023
- Once a security-impactful issue has been scored, if it exceeds a threshold, security advisories are issued.
  - Juniper issues security advisories (JSAs) when the score is ≥ 5.0.
  - Juniper currently publishes both CVSS v4.0 and v3.1 scores, but will slowly deprecate v3.1 scores as industry adoption of CVSS v4.0 increases.

What can and can’t be said in a security advisory (SIRT controls the message)

“The official Juniper Networks statement regarding any vulnerability is exclusively the Juniper Security Advisory (JSA) published by the Juniper SIRT. Any supplemental information regarding a SIRT PR or JSA, provided by any other group within Juniper Networks, is explicitly forbidden. Information about product security vulnerabilities is the most critically confidential information we as Juniper Networks employees hold secret, and sharing strictly confidential information is in direct violation of Juniper's Worldwide Code of Business Conduct and Ethics.”

BGP and CVSS

... the path to ≥ 5.0

Network Protocols Score High

- Issues impacting routing protocols typically impact the CVSS attribute of *Availability*.
  - The CVSS v4.0 impact metric for Availability has been decompressed into Availability Impact to the Vulnerable System (VA) and Subsequent Systems (SA)
  - The system may continue running, but routing may malfunction, peering sessions/adjacencies may drop. “You can’t get there from here…”
  - Even worse, the system may crash impacting many resources accessed through that system.
  - Depending on the “attack”, the impact on availability may be “low” because you consider it “temporary” or ”high” because you consider it sustained.

Network Protocols Score High (2)

- *Attack Complexity* is typically “low” for many routing protocol issues.
  - If you’re able to generate routing protocol traffic that can be received by the impacted system, this isn’t “high”.
  - Some protocols are easier to attack than others. BGP, in particular, can be “easy” to attack.

Network Protocols Score High (3)

- The majority of routing protocol bugs do not impact *Integrity*.
  - This is lucky. Integrity would tend to mean that things outside of routing are impacted.
  - Or, that the attacker can arbitrarily modify the routing protocol information itself to their own whims, then a higher CVSS will result.
    - In CVSS 4.0 the concept of “trustworthiness and veracity of information” is introduced. In CVSS 3.1 this is “modification of data”.
  - For CVSS 3.1 you may have no integrity impact; but in a CVSS 4.0 world you may see Integrity impact being scored because the information is untrustworthy.

Network Protocols Score High: Examples

CVSS 3.1:

Attack Vector: Network;
Attack Complexity: Low;
Privileges Required: None;
User Interaction: None;
Scope: Unchanged;
Confidentiality: None;
Integrity: None

- Availability: Low… Score is 5.3 (Medium) https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Availability: High… Score is 7.5 (High!) https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - **“Ye Olde DoS”. CVSS 7.5 is the most common score for a networking product. Send this thing and it crashes the box.**

When is a bug just a bug and not a security issue?

Is it bad enough?

- Jeff's rule for routing protocols:
  "Can I cause bad behavior by sending a packet?"
- Derrick Scholl's (Juniper SIRT Sr. Director) rule for whether something should be covered by a security advisory (disclosure):
  "If an attacker knew all the details, could they make a bad thing happen on purpose?"

Tug of war between severity and risk

- The first question an operator wants to know is, “am I exposed?”
  - Part of the answer depends on what the “blast radius” is for the issue.
- Issues that may be “local”, say between two routers, may have high severity, but *may* be acceptable risk for some operators.
- Many issues for BGP mean that Internet exposure is enough to make them vulnerable.

Given how easily BGP scores high, why aren’t there more security advisories?

There should be more…

- In some respects, a vendor's willingness to issue security advisories shows that it has crossed a threshold of a healthy software development life-cycle (SDL). Security is part of the process!
- Smaller vendors may not have the resources to manage the security aspects of their SDL. They may also not have people that recognize the severity of their issues and impact on their customer base.
  - Vendors are not all equal and do not serve the same segments. (Internet vs. Data Center, e.g.)

There are perverse disincentives

- The “wall of silence” for an advisory creates a culture of fear.
- Network element upgrades are operationally disruptive and may be expensive.
- There are revenue impacts from appearing to have ”more vulnerabilities”. This pressures organizations to hide the severity of issues.

Sometimes it’s a matter of perspective

- Training software engineers to write secure code involves teaching them to think about vulnerabilities.
- Learning a “security mindset” is hard.
- The training requires analyzing a bug after the fact for security implications.

What we've seen

- Not everyone likes NVD's CVE program or FIRSTs CVSS
  - Revenue may be impacted
  - May only issue CVEs when threated with disclosure
  - May use lower "CVE counts" to create a marketing perception of "better security posture" of a vendor
- There are other/emerging standards – SBOM, SBOM VEX, EPSS, VISS
  - Confusing to consumers
- Sometimes competing standards – a project to generate a unique non-NVD CVE ID was launched.

Bridging the gap between severity and risk

CVSS updates

- CVSS 4.0 was published on November 1, 2023 and is currently being used by several vendors.
- NVD and CVE.org have begun publishing v4.0 scores provided by vendors.
- Better granularity for severity inputs for network protocols now exists.

CVSS updates (2)

- **Scope** is gone! Vulnerable system and Subsequent system impact metrics are more clearly defined.
- Better supplemental metrics, importantly, **Provider Urgency** (U) now exists (Clear, Green, Amber, Red)
- Threat Metrics now introduced! Includes **Exploit Maturity** (E) – Attacked, or Proof of Concept

A better framework for discussing risk

- CVSS is intended for severity.
- There is a need for a consistent framework to discuss risk, especially for networking products and protocols.
- CVE provides some of the utility for this toolbox but is insufficient.
- Customers should expand upon the vendor-supplied CVSS scores.
- Use CVSS + EPSS + VISS as inputs to your risk management system.

Reducing risk in BGP

Things in BGP

- RFC 7606 error handling procedures have reduced some of the impacts of the protocol being rigid.
- BGP has been a successful protocol because its extensions have been easy to incrementally deploy.
  - Those same mechanisms create opportunity for large blast radius.
  - BGP is used for far more things today than just Internet (and just BGP).

Things in BGP (2)

- Discussion is happening in IETF about risk reduction by design:
  - Attribute and route property scoping.
  - Sandboxing new features under a new address family. (But what to do when you can't use structural separation and those features *must* run on routers that do other important things?)
  - "Attribute escape" https://datatracker.ietf.org/doc/draft-haas-idr-bgp-attribute-escape/

Contributions

- Thanks to Dave Dugal, co-chair of the CVSS SIG, for his review and commentary on this presentation.

Thank you

NANOG™