



# Black and Blue or White and Gold?

Minimizing Vulnerability Scoring Discrepancies due to Limited Information

Michael Schueler  
Incident Manager, Cisco PSIRT

VulnCon 2024 – 27 March 2024

# Speaker Background

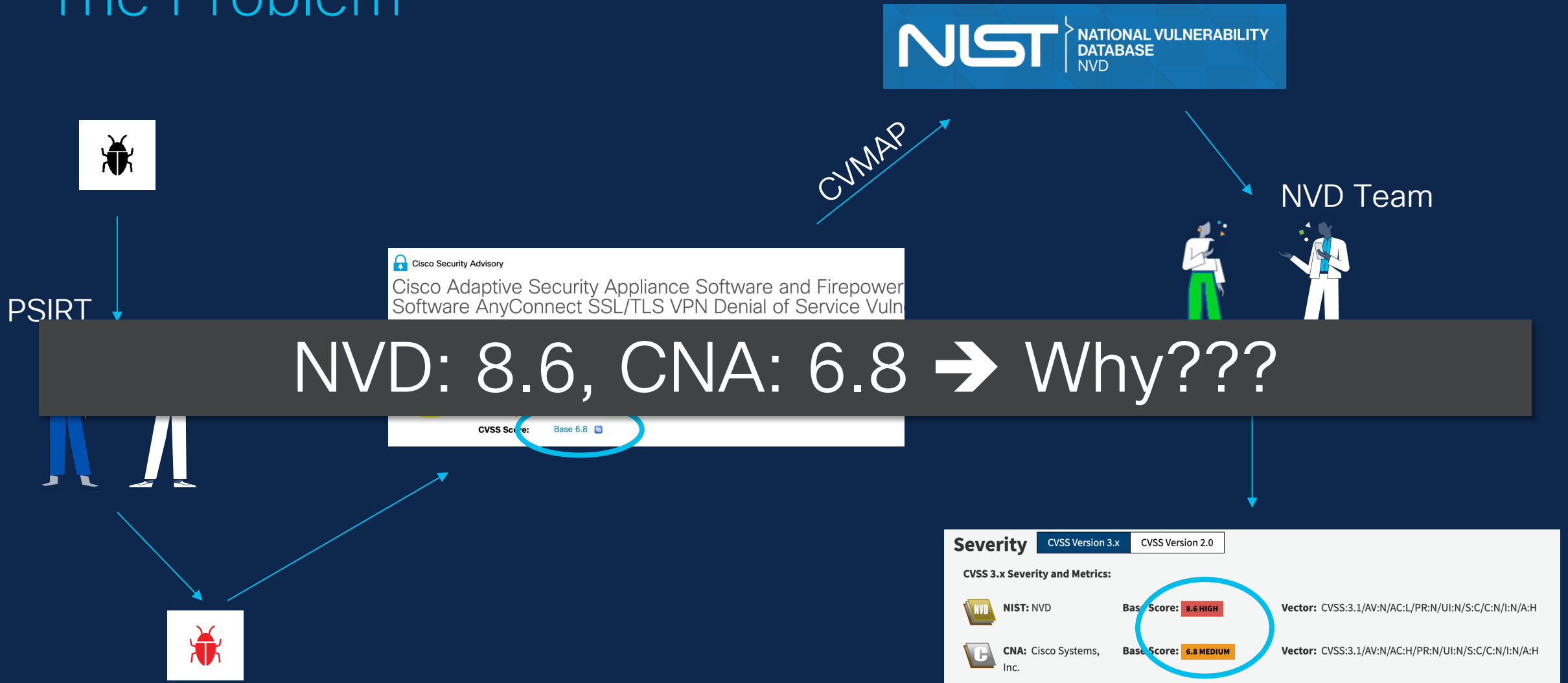
Michael Schueler, Incident Manager, Cisco PSIRT

- With Cisco since 2007, PSIRT since 2016
- M.Sc. level degree from RWTH Aachen University
- CCIE, CISSP, and GCIH certifications
- Handling the most challenging, complex, and impactful vulnerabilities and compromises

# The Dress




# The Problem




# Data Analyzed

## CVSS v3.1 Statistics for Cisco Systems, Inc. as of 10/06/2023

Total Number CVEs Submitted	194	Number of Metrics Compared	320
Total Number CVEs Reviewed	40	Analyst Match Count	291
Acceptance Level	 Contributor	Match Percent	90.9

↳ 29 metrics require analysis

## CVSS v3.1 Statistics for Cisco Systems, Inc. as of 11/15/2023

Total Number CVEs Submitted	1271	Number of Metrics Compared	320
Total Number CVEs Reviewed	40	Analyst Match Count	277
Acceptance Level	 Contributor	Match Percent	86.6

↳ 43 metrics require analysis

# Metric Statistics Analysis

Identifying the Best Match Based on Vulnerability Facts



→ Focus on the “Unclear” ones!

■ Cisco ■ NVD ■ Unclear

Oct 6, 2023



■ Cisco ■ NVD\* ■ Unclear

Nov 15, 2023

\* NVD score correct, as Cisco score taken from advisory level, not CVE level (tooling limitation until mid July 2023)

# Cisco Firepower Threat Defense Software Snort 3 Geolocation IP Filter Bypass Vulnerability



**Medium**

Advisory ID: [cisco-sa-ftdsnort3sip-bypass-LMz2ThKn](#) CVE-2023-20267 [Download CSAF](#)

First Published: 2023 November 1 16:00 GMT CWE-284 [Email](#)

Version 1.0: [Final](#)

Workarounds: [Yes](#)

Cisco Bug IDs: [CSCwe69833](#)

CVSS Score: [Base 4.0](#)

### Summary

A vulnerability in the IP geolocation rules of Snort 3 could allow an unauthenticated, remote attacker to potentially bypass IP address restrictions.

This vulnerability exists because the configuration for IP geolocation rules is not parsed properly. An attacker could exploit this vulnerability by spoofing an IP address until they bypass the restriction. A successful exploit could allow the attacker to bypass location-based IP address restrictions.

## Severity

CVSS Version 3.x CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

	<b>NIST:</b> NVD	<b>Base Score:</b> 5.3 MEDIUM	<b>Vector:</b> CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
	<b>CNA:</b> Cisco Systems, Inc.	<b>Base Score:</b> 4.0 MEDIUM	<b>Vector:</b> CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N

# Reasons for Scoring Discrepancies

- Insufficient information in textual CVE description
- Textual description focuses on technical detail rather than outcome
- Limited product knowledge at NVD
  - NVD analysts cover thousands of products across hundreds of vendors
- CVSS specification interpretation differences



# Cisco PSIRT's Improvement Plan

Within the Advisory/CVE Summary:

- Explain why attack complexity is “High”
- Make the required privilege level explicit
- Explain reasoning for scope change
- Add context to corner cases
- Focus on outcome rather than technical detail
- Ensure summary is understandable even with little product knowledge



# Observed Scoring Mistakes & Derived Best Practices

- SSH/Telnet **pre-auth** issues
  - Attack Vector is **Network** (AV:N)
  - SSH/Telnet **post-auth** issues typically are Attack Vector **Local** (AV:L)
- **Persuading** a user to do something implies user interaction
  - User Interaction **Required** (UI:R) in CVSSv3.1
  - User Interaction **Active** (UI:A) in CVSSv4.0



# CVSS Specification Interpretation Differences

- Does security policy (e.g., ACL) bypass imply S:C and I:L?
  - Resource behind the device are either no longer protected or become unreachable
  - Is the protected “network” a security boundary?
- Does admin-level credentials required (PR:H) typically imply A:N
  - Admin can disable interfaces/services by design
  - Need to score based on privileges gained, not attained
  - Are different methods to achieve the same outcome “privileges gained”?

➔ Actively discussed in the FIRST CVSS SIG  
➔ “Thank you Nick Leali and Chris Turner!”



# Q&A



# Resources

- The Dress  
[https://en.wikipedia.org/wiki/The\\_dress](https://en.wikipedia.org/wiki/The_dress)
- Common Vulnerability Scoring System  
<https://www.first.org/cvss/>
- CVE Program  
<https://www.cve.org>
- Cisco Security Advisories  
<https://sec.cloudapps.cisco.com/security/center/publicationListing.x>
- NVD CVSS v3.1 Statistics for Cisco Systems, Inc.
  - As of 10/06/2023: <https://nvd.nist.gov/vuln/cvmap/report/12896>
  - As of 11/15/2023: <https://nvd.nist.gov/vuln/cvmap/report/13635>



The bridge to possible