

GRC Controls for the CVE Gap

What Is It and How to Manage It

January 13, 2025



Introduction

- The CVE gaps in this presentation are identified as:
 - CPE naming inconsistencies
 - NVD backlog of CVE enrichment
- Primary opportunity statement:
 - Managing or reducing impacts of unknown risks
- GRC controls vary throughout People, Process, and Technology domains.
 - GRC controls in this presentation are tailored for the described CVE gaps.
- The concepts in this presentation may or may not apply to your organization and is intended to be a guide. Each must be assessed for applicability to your environment.



**Common
Vulnerabilities &
Exposures**

1) What are the CVE Gaps?

- Common Vulnerabilities and Exposures (CVE)
 - a crucial source of information on cyber vulnerabilities for organizations and malicious actors alike.
 - The CVE Numbering Authorities (CNA), CVE.org, MITRE, and the National Institute of Standards and Technology (NIST) collaborate to identify and publish known cyber vulnerabilities, helping organizations protect their environments.
- Specifically, one of the NVD's responsibilities is to enrich initial CVE details with:
 - Definitions:
 - Common Platform Enumeration (CPE): A dictionary of hardware, operating systems, and applications.
 - Common Vulnerability Scoring System (CVSS): A system for measuring the severity of software vulnerabilities.
 - Common Weakness Enumeration (CWE): A taxonomy for identifying common sources of software flaws (e.g., buffer overflows, input validation failures).
 - The NVD is under a significant backlog to enrich CVE data

The Gaps:

1. Enriched CVE data by NVD are critical for organizations to identify and manage known cyber vulnerabilities but CPE data may not be identifiable
2. The NVD is in a current backlog to enrich CVE data and face several challenges. The risks need to be assessed and evaluated.

2.1) Scenario Example

Two new vulnerabilities are found by a CNA one month apart for ACME Industries

ACME Industries	Vulnerability #1	Vulnerability #2
Date Identified	January 1	February 1
CPE Vender Name	ACME	ACME Industries
CPE Product Name	Good Trap v1.2.3	Good Traps v1.2.3
CVSS	8.1	8.1
CWE	Security flaw 1.1	Security flaw 2.2
Date Released	January 7	February 7

The CPE vendor name and product name could be named differently from prior vulnerabilities.

2.2) CPE Example

	(CNA) Red Hat	cve.org
Vulnerability ID	RHSA-2024:4312 - Security Advisory	CVE-2024-6387
Date Published	2024-07-03	2024-07-01
CVSS	8.1 (Important)	8.1 (High)
Vendor	Red Hat, Inc	redhat
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64	rhel_eus:9.2
Risk	Is the vulnerability tool looking for: <ul style="list-style-type: none">• vendor matches of “Red Hat, Inc” or “redhat”?• affected products matches of “... support 9.4 x86_64” or “rhel_eus:9.2”?	

Sources:

<https://access.redhat.com/errata/RHSA-2024:4312>

<https://www.cve.org/CVERecord?id=CVE-2024-6387>

2.2) CPE Example (con't)

```
{
  "dataType": "CVE_RECORD",
  "cveMetadata": {
    "cveId": "CVE-2024-6387",
    "assignerOrgId": "53f830b8-0a3f-465b-8143-3b8a9948e749",
    "state": "PUBLISHED",
    "assignerShortName": "01T12:37:25.431Z",
    "dateUpdated": "2024-11-24T17:19:20.471Z",
    "containers": {
      "cna": {
        "title": "Openssh: regresssion - race condition in ssh allows rce/dos",
        "value": "Important",
        "namespace": "https://access.redhat.com/security/updates/classification/",
        "type": "Red Hat severity rating",
        "cvssV3_1": {
          "attackComplexity": "HIGH",
          "attackVector": "NETWORK",
          "availabilityImpact": "HIGH",
          "baseScore": 8.1,
          "baseSeverity": "HIGH",
          "confidentialityImpact": "HIGH",
          "S": 3.1,
          "AV": "N",
          "AC": "H",
          "PR": "N",
          "UI": "N",
          "S": "U",
          "C": "H",
          "I": "H",
          "A": "H",
          "version": "3.1",
          "format": "CVSS"
        },
        "descriptions": [
          {
            "lang": "en",
            "value": "A security regression (CVE-2006-5 in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period."
          }
        ],
        "affected": [
          {
            "status": "affected",
            "version": "8.5p1",
            "versionType": "custom",
            "lessThanOrEqual": "9.7p1",
            "packageName": "OpenSSH",
            "collectionURL": "https://www.openssh.com/changelog.html",
            "collectionURL": "https://access.redhat.com/downloads/content/package-browser/",
            "packageName": "openssh",
            "defaultStatus": "affected",
            "versions": [
              {
                "cpe": "o:redhat:enterprise_linux:9::baseos",
                "cpe": "a:redhat:enterprise_linux:9::appstream",
                "vendor": "Red Hat",
                "product": "Red Hat Enterprise Linux 9 browser/",
                "packageName": "openssh",
                "defaultStatus": "affected",
                "versions": [
                  {
                    "version": "0:8.7p1-38.el9_4.1",
                    "lessThan": "*",
                    "versionType": "rpm",
                    "status": "affected",
                    "vendor": "Red Hat",
                    "product": "Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions",
                    "collectionURL": "https://access.redhat.com/downloads/content/package-browser/",
                    "packageName": "openssh",
                    "defaultStatus": "affected",
                    "versions": [
                      {
                        "cpe": "a:redhat:rhel_e4s:9.0::appstream",
                        "cpe": "o:redhat:rhel_e4s:9.0::baseos",
                        "vendor": "Red Hat",
                        "product": "Red Hat OpenShift Container Platform 4.13",
                        "collectionURL": "https://catalog.redhat.com/software/containers/",
                        "packageName": "rhcos",
                        "defaultStatus": "affected",
                        "versions": [
                          {
                            "version": "413.el8",
                            "cpe": "a:redhat:openshift:4.13::el8",
                            "cpe": "a:redhat:openshift:4.13::el9"
                          },
                          {
                            "version": "414.el8",
                            "cpe": "a:redhat:openshift:4.14::el8",
                            "cpe": "a:redhat:openshift:4.14::el9"
                          },
                          {
                            "version": "415.el8",
                            "cpe": "a:redhat:openshift:4.15::el8",
                            "cpe": "a:redhat:openshift:4.15::el9"
                          }
                        ]
                      }
                    ]
                  }
                ]
              }
            ]
          }
        ]
      }
    }
  }
}
```

Source:

JSON page for CVE-2024-6387 (Captured on 2025-01-12)

<https://cveawg.mitre.org/api/cve/CVE-2024-6387>

2.3) NVD Backlog Example

	(CNA) Cisco	cve.org
Vulnerability ID	RHSA-2024:4312 - Security Advisory	CVE-2014-2120
Date Published	2014-03-18	2014-03-19
Date Revised	2024-12-02	2015-05-04
CVSS	4.3 (Important)	5.4
Vendor	Cisco Systems, Inc	cisco
Affected Products	Cisco Adaptive Security Appliance (ASA) Software	adaptive_security_appliance_software
Risk	Is the Vulnerability Management (VM) tool looking at NVD for CVE updates or the CNA? <ul style="list-style-type: none">• If the CNA, then VM should have received an alert on Dec 02, 2024 of an update• If the NVD, then no VM alert would have been triggered on Dec 02, 2024	

Sources:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CVE-2014-2120>

<https://www.cve.org/CVERecord?id=CVE-2014-2120>



2.3) NVD Backlog Example (con't)



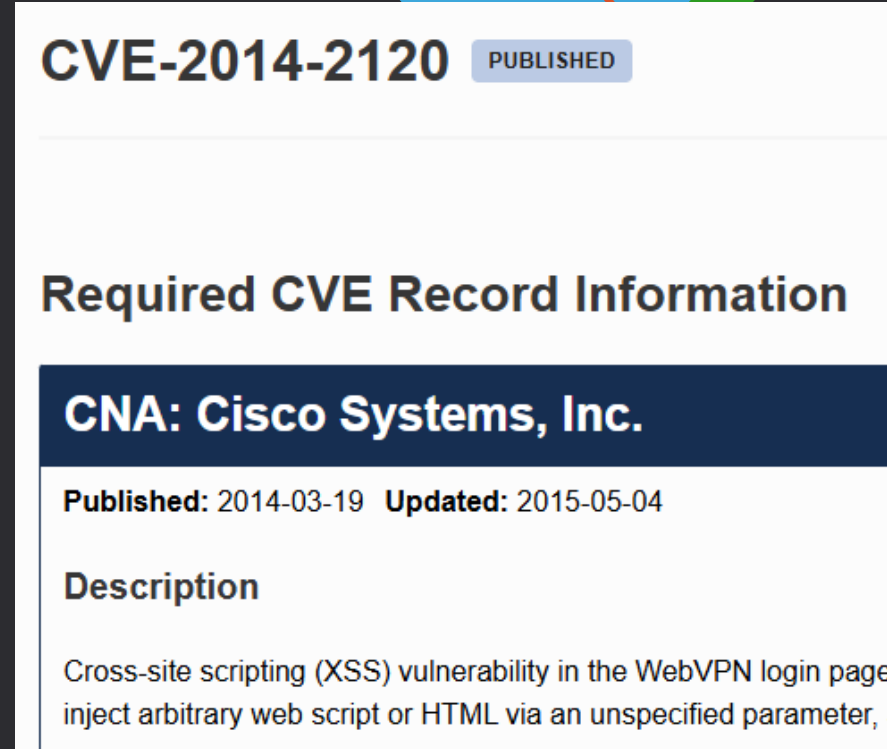
The screenshot shows the Cisco Security Advisory page for CVE-2014-2120. The page title is "Cisco Adaptive Security Appliance WebVPN Vulnerability". A yellow circle highlights the "Medium" severity rating. The advisory ID is "cisco-sa-CVE-2014-2120" and "CVE-2014-2120". The first published date is "2014 March 18 16:00 GMT" and "CWE-79". The last updated date is "2024 December 2 20:05 GMT". The version is "1.1: Final". There are no workarounds available. The Cisco Bug ID is "CSCun19025" and the CVSS score is "Base 4.3, Temporal 3.4".

Medium

Advisory ID: cisco-sa-CVE-2014-2120 CVE-2014-2120
First Published: 2014 March 18 16:00 GMT CWE-79
Last Updated: 2024 December 2 20:05 GMT
Version 1.1: Final
Workarounds: No workarounds available
Cisco Bug IDs: CSCun19025
CVSS Score: Base 4.3, Temporal 3.4

Summary

A vulnerability in the WebVPN login page of Cisco Adaptive Security Appliance allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. An attacker could use this vulnerability to inject arbitrary web script or HTML via an unspecified parameter, which could be used to compromise the user of WebVPN on the Cisco ASA.



The screenshot shows the CVE record for CVE-2014-2120 on CVE.org. The record is marked as "PUBLISHED". The required CVE record information is displayed, including the CNA: Cisco Systems, Inc. The record was published on 2014-03-19 and updated on 2015-05-04. The description states: "Cross-site scripting (XSS) vulnerability in the WebVPN login page allow an unauthenticated, remote attacker to inject arbitrary web script or HTML via an unspecified parameter, which could be used to compromise the user of WebVPN on the Cisco ASA."

CVE-2014-2120 PUBLISHED

Required CVE Record Information

CNA: Cisco Systems, Inc.

Published: 2014-03-19 **Updated:** 2015-05-04

Description

Cross-site scripting (XSS) vulnerability in the WebVPN login page allow an unauthenticated, remote attacker to inject arbitrary web script or HTML via an unspecified parameter, which could be used to compromise the user of WebVPN on the Cisco ASA.

Sources:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CVE-2014-2120>

<https://www.cve.org/CVERecord?id=CVE-2014-2120>

(Captured on 2025-01-12)

3) What are the Risks?

1. Are all applicable vulnerabilities appropriately identified?
 - Most vulnerabilities are identified with automated tools. How many are not identified due to the CPE issue? What is your organization's risk appetite?
 - Evaluate your vulnerability tools to understand the dependence on CPEs to identify applicable CVEs
 - Are the CNAs leveraged?
2. If gaps are discovered, how can your organization protect against unknown risks?
 - How does your organization manage unknown cyber risks?
 - What are the probabilities that malicious actors understand the potential risks?
 - What is the timeframe for the needed protection to unknown risks?
3. NVD holds a backlog of enriching CVE information which includes CPE, CVSS, and CWE
 - When are applicable CVEs to your environment to be published with enriched data?
 - Is your organization vulnerable to unknown CVEs?

4) How Will This Gap be Fixed?

- A group of international professionals have investigated a solution but it will take time and resources
 - CVE.org is investigating the implementation of purl to replace CPEs
 - The following working groups directly discuss the gaps:
 - Software Bill of Materials (SBOM) Working Group
 - Vulnerability Database Working Group
- Contact Tom Alrich for more information or how to contribute to the solution
 - tom@tomalrich.com

5) GRC Controls to Reduce Risk

1. Understand your dependencies on the NVD.
2. Review your resiliency program for NVD and CVE dependencies.
3. Execute risk management processes on your NVD and CVE dependencies.
4. Enhance cyber security controls and business processes for monitoring critical systems.

More details are provided in our blog on the topic:

<https://simpligr.com/2024/10/29/grc-controls-for-the-nvd-issue/>

5.1) GRC Controls – Dependencies

1. Understand your dependencies on the NVD.
 - Engage with your vulnerability management sources to understand the dependencies.
 - Review the impacts of the dependencies to your critical processes and assets.
 - Analyze the outcomes of these discussions and assess the risks.
 - Review your existing people, process, and technology controls with updated scenarios
 - Update the residual risks
 - Complete a gap analysis
 - Communicate the findings, positive or negative

5.2) GRC Controls – Resiliency

2. Review your resiliency program for NVD dependencies.

- Update your Business Impact Analysis (BIA) and value chain assessments.
- Review your Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for potential triggers.
- Practice your Cyber Security Incident Response Plan (CSIRP).
- Increase the frequency of testing backups for critical systems.
- Conduct more frequent incident response tabletop exercises excluding known vulnerabilities.

5.3) GRC Controls – Risk Management

3. Execute risk management processes on your NVD dependencies.

- Implement temporary monitoring controls for supply chain vendors with access to critical systems.
- Identify and monitor compensating controls to reduce risk and respond.
- Update threat models excluding CVE data.

5.4) GRC Controls – Monitoring

4. Enhance cyber security controls and business processes for monitoring critical systems.

- Update business processes for monitoring critical systems from resiliency and risk activities
- Ensure authorized baselines are updated for acceptable traffic.
- Increase log monitoring for critical systems.
- Configure SIEM to alert on newly assessed risks.
- Vendors actively engages as CNA providers will often supply security patches or workarounds on their websites. Try to implement security patches with more diligence versus dependence on mitigations or exceptions. While Vendors offering varying degrees of vulnerability exposures on their website, you should independently assess your exposure via BIA and asset criticality analysis.

6) What are the Opportunities

1. Implement proactive controls
2. Flexibility and scalability for the GRC solutions
3. Foundational solutions
4. Update your BIA and BCP programs



7) Self-Assessment Questions

1. What is my organization's risk appetite on the NVD backlog?
2. What is my dependency on vulnerability tools that rely on CPE data?
3. If an incident were to occur, are we ready to respond?
4. Do we have all our critical assets monitored in relation to risk?

8) How SimpliGRC Can Support

GRC solutions across regulations, frameworks, and standards

Successfully completed several assessments and audits including NIST CSF, CIP, CIS, ISO, TSA

Diverse range of different IT and OT environments and industries

Expert process development and re-engineering

Senior analysis and project management services

Softening silos and sub-cultures to achieve enterprise or project goals

Strategy development and implementation

Experienced in Business Impact Analysis and Risk Assessments

The managing directors deliver the services to offer the direct experience and competencies

Local to Calgary and Edmonton in Alberta, Canada



Contact Us

For more information:

visit <https://simpligrc.com>

OR

email: info@simpligrc.com

Blog: [GRC Controls for the NVD Issue](#)



THANK YOU