IT NATION™ SECURE

hosted by CONNECTWISE

Vulnerability Management: Why you need it and how does ConnectWise support you

Tammy Cohn, Sr. Product Manager

Tammy.cohn@connectwise.com

IT NATION™ SECURE

Agenda

1 What is Vulnerability Management?

2 Vulnerability Management - Key Components

3 Vulnerability Management Benefits

4 Remediation Feature- Demo

5 A Glance into the Roadmap

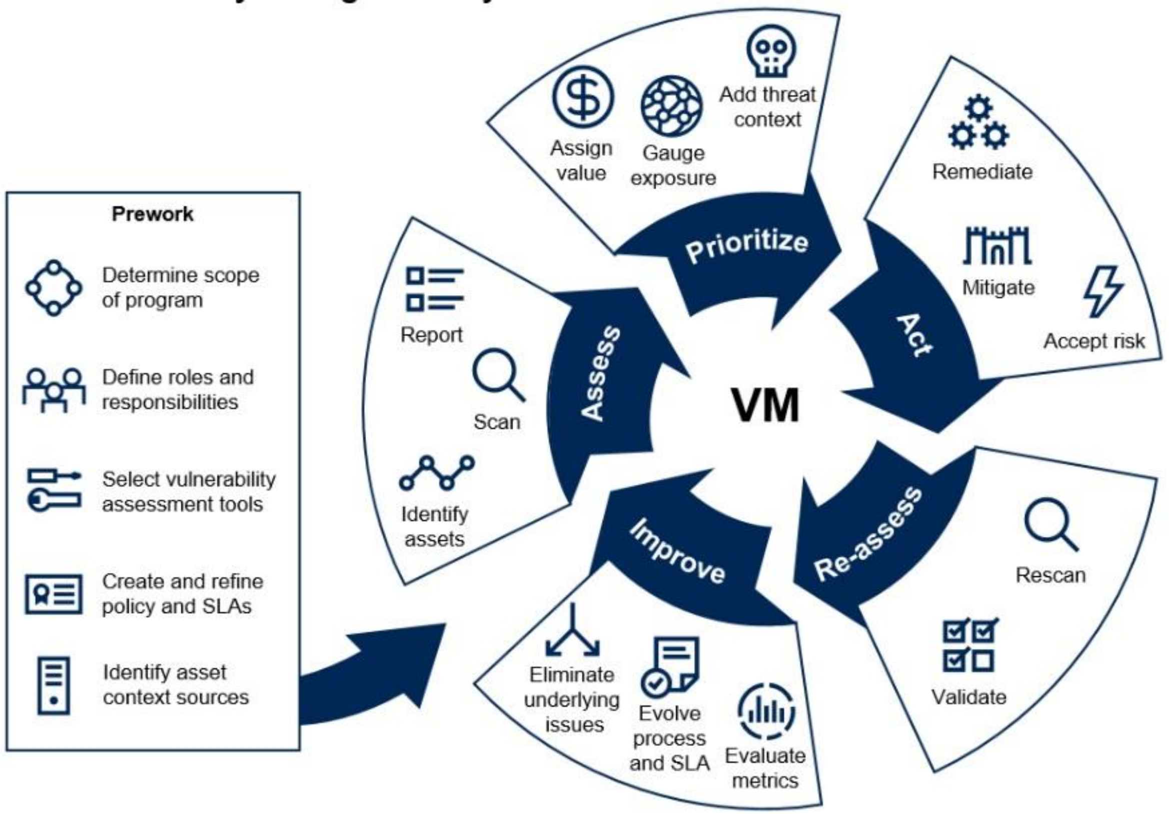
6 Q&A

What is Vulnerability Management ?

Vulnerabilities are weaknesses in software or hardware that can be exploited by attackers to gain access to an organization's systems.

Vulnerability Management is a continuous process of identifying, assessing, prioritizing, and mitigation vulnerabilities in an organization's IT infrastructure. Its main goal is to reduce the prevalence and impact of vulnerabilities and exploitable conditions across organization's IT infrastructure and technologies.

The Vulnerability Management Cycle



Source: Gartner
ID: 410271

Vulnerability Management – Key Components

Vulnerability Identification: Using automated tools and manual assessments to discover vulnerabilities in systems and networks

Vulnerability Assessment: Evaluation the severity and impact of the identified vulnerability

Risk Prioritization: Determining priorities based on the criticality and potential impact of vulnerability

Remediation: Applying necessary patches, fixes, or mitigations to address vulnerabilities

Vulnerability Management Benefits

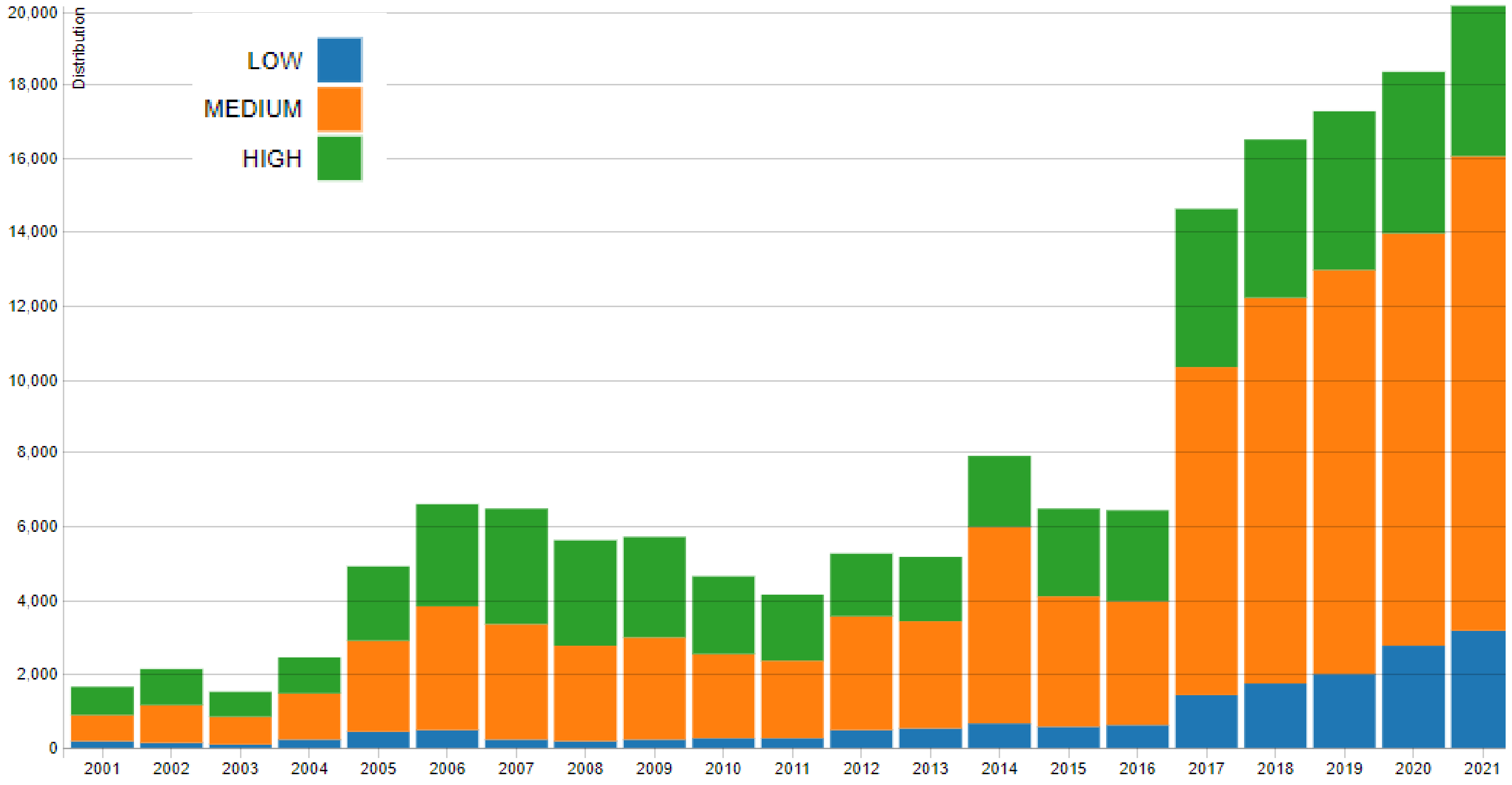
An effective vulnerability management program allows you to:

- Move from reactive to proactive risk mitigation
- Enhance client’s trust
- Support compliance and regulatory requirements
- Reduce costs by avoiding security breaches, data loss, and reputational damage.

Why is Vulnerability Management needed ?

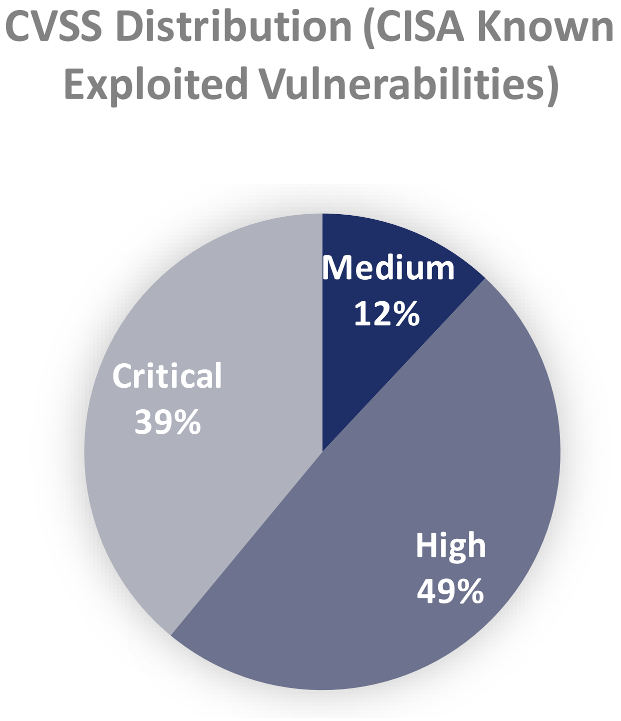
Vulnerability Management in Numbers

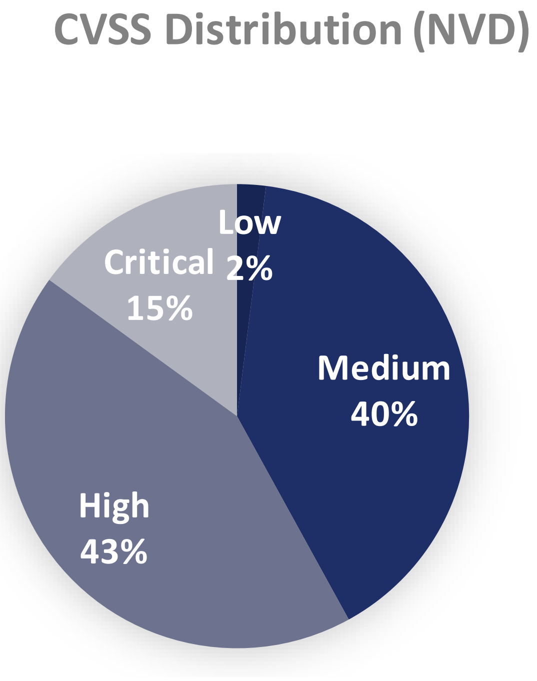
CVSS Severity Distribution Over Time



Source: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

Vulnerability Management in Numbers

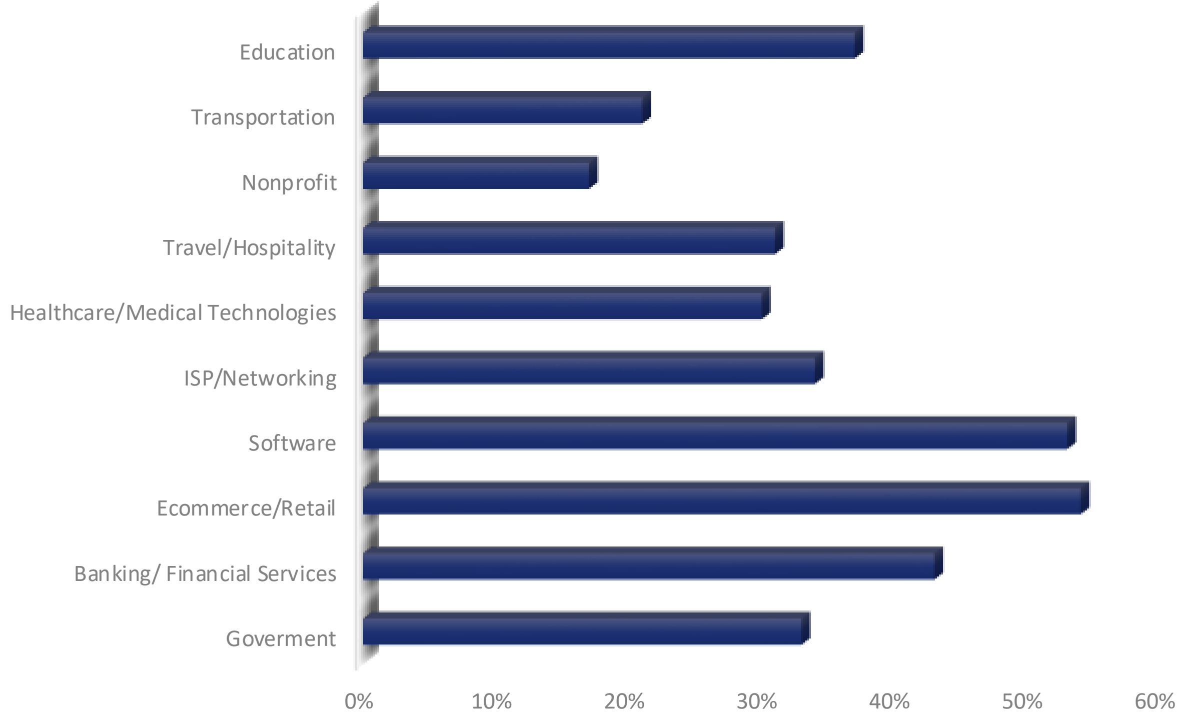




https://nucleussec.com/blog/top-observations-from-cisa-kev-enrichment-dashboard/

Vulnerability Management in Numbers

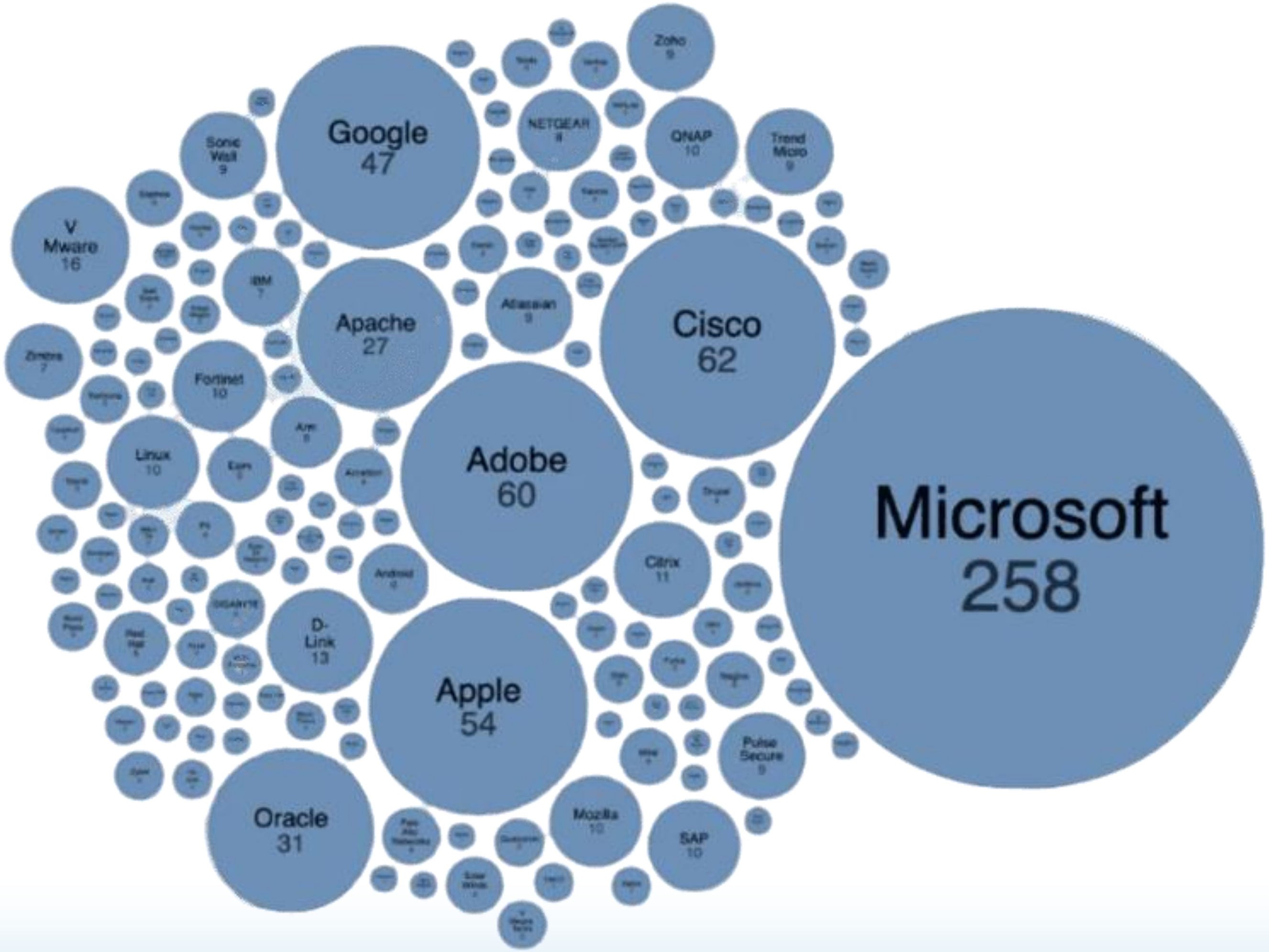
Hackers Focus in 2022 by Industry



https://www.traceable.ai/blog-post/hackerone-2022-hacker-powered-security-report

CISA Known Exploited Vulnerabilities by Vendor

Vulnerability Management in Numbers



Vulnerability Management in Numbers

$4.35 M

Average data breach cost in 2022

Vulnerability Management in Numbers

95%

Of Breaches are caused by human error

Vulnerability Management in Numbers

65%

Of Customers would lose trust in a company experiencing a data breach

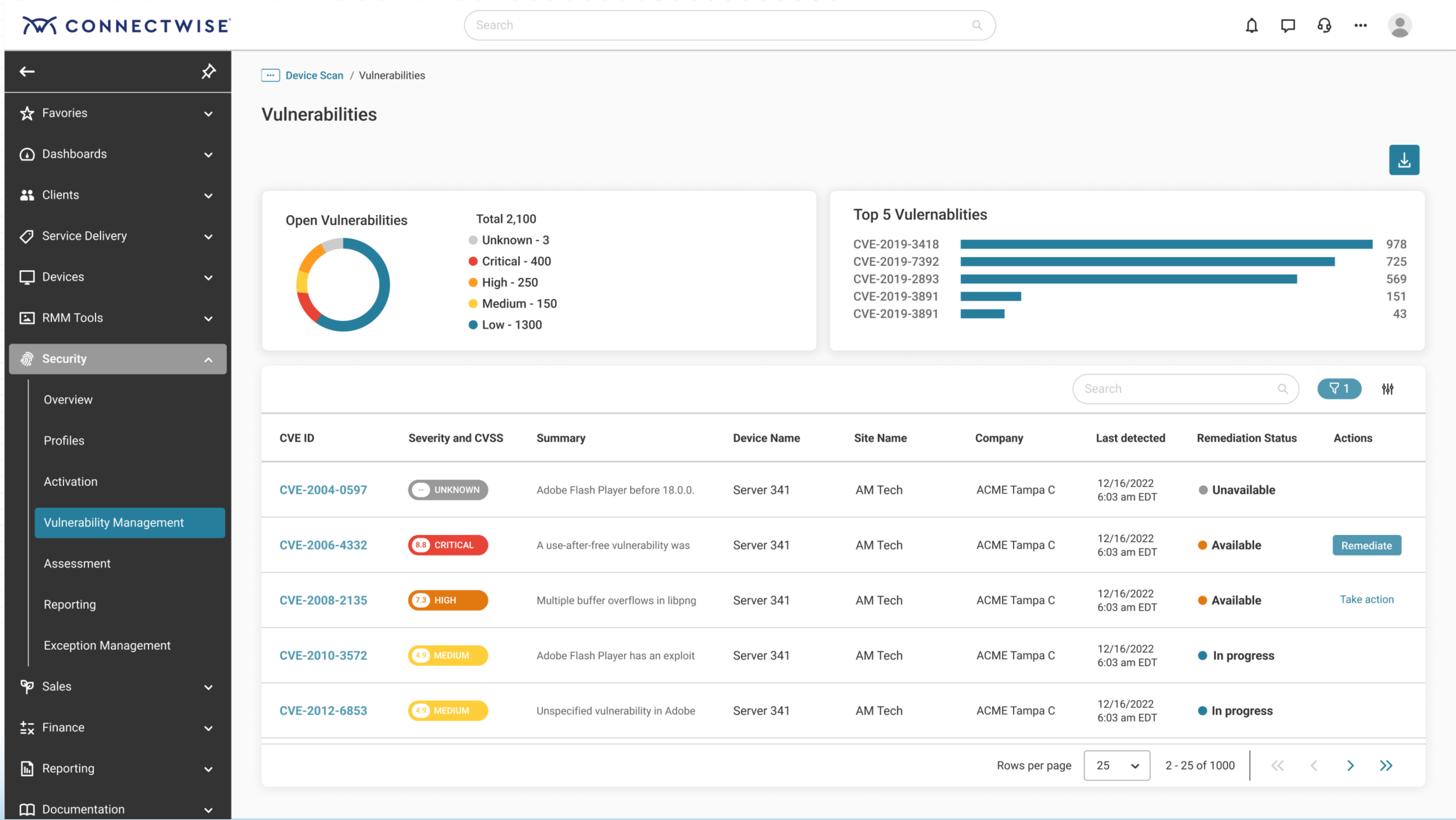
Why ConnectWise Vulnerability Management ?

- Centralized Platform (Asio)
- Integration with ConnectWise patch management
- Comprehensive Vulnerability Assessment
- Scalability & Flexibility
- Industry Leading Expertise

CHECK

ConnectWise Vulnerability Management - Demo

Demo



CONNECTWISE

Search

Device Scan / Vulnerabilities

Vulnerabilities

Open Vulnerabilities

Total 2,100

- ● Unknown - 3
- ● Critical - 400
- ● High - 250
- ● Medium - 150
- ● Low - 1300

Top 5 Vulnerablities

CVE-2019-3418	978
CVE-2019-7392	725
CVE-2019-2893	569
CVE-2019-3891	151
CVE-2019-3891	43

Search

CVE ID	Severity and CVSS	Summary	Device Name	Site Name	Company	Last detected	Remediation Status	Actions
CVE-2004-0597	-- UNKNOWN	Adobe Flash Player before 18.0.0.	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Unavailable	
CVE-2006-4332	8.8 CRITICAL	A use-after-free vulnerability was	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Available	Remediate
CVE-2008-2135	7.3 HIGH	Multiple buffer overflows in libpng	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Available	Take action
CVE-2010-3572	4.9 MEDIUM	Adobe Flash Player has an exploit	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	
CVE-2012-6853	4.9 MEDIUM	Unspecified vulnerability in Adobe	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	

Rows per page 25 2 - 25 of 1000

Recording-20230509_153020.webm

Development Horizons

Short Term

- ✓ Vulnerability Remediation tracking
- ✓ WindowsOS Automated Vulnerability patching
- Exception management
- Advanced scan scheduling
- Vulnerability centric monitoring

Mid Term

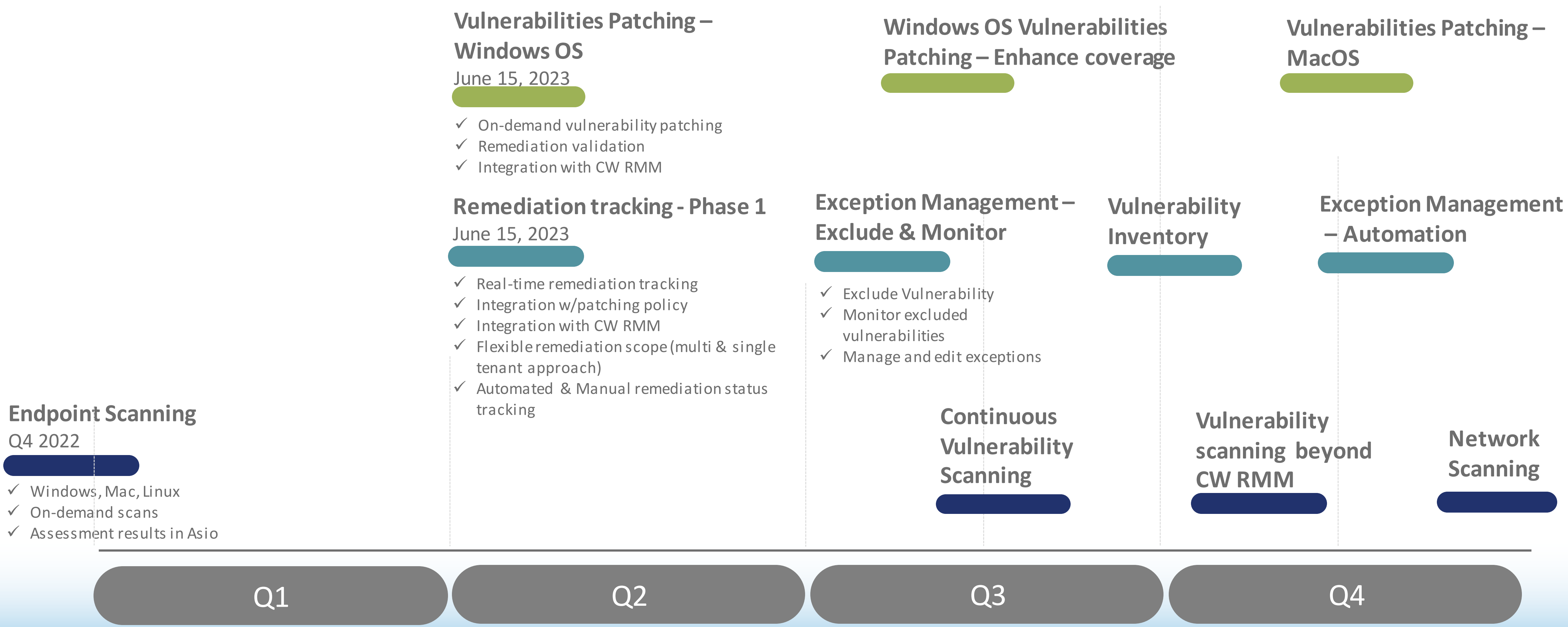
- Risk-base Vulnerability Prioritization
- Network vulnerability scanning
- MacOS Automated Vulnerability patching

Long Term

- Vulnerability Management across non CW scanners
- Advance reporting
- Policy & Compliance
- Asset management
- Cloud Support
- …

Vulnerability Management – 2023 Roadmap

Vulnerability Patch Management | Vulnerability Scanning | Vulnerability Remediation Management



Endpoint Scanning
Q4 2022

- ✓ Windows, Mac, Linux
- ✓ On-demand scans
- ✓ Assessment results in Asio

Vulnerabilities Patching – Windows OS
June 15, 2023

- ✓ On-demand vulnerability patching
- ✓ Remediation validation
- ✓ Integration with CW RMM

Remediation tracking - Phase 1
June 15, 2023

- ✓ Real-time remediation tracking
- ✓ Integration w/patching policy
- ✓ Integration with CW RMM
- ✓ Flexible remediation scope (multi & single tenant approach)
- ✓ Automated & Manual remediation status tracking

Windows OS Vulnerabilities Patching – Enhance coverage

Exception Management – Exclude & Monitor

- ✓ Exclude Vulnerability
- ✓ Monitor excluded vulnerabilities
- ✓ Manage and edit exceptions

Continuous Vulnerability Scanning

Vulnerability Inventory

Vulnerability scanning beyond CW RMM

Vulnerabilities Patching – MacOS

Exception Management – Automation

Network Scanning

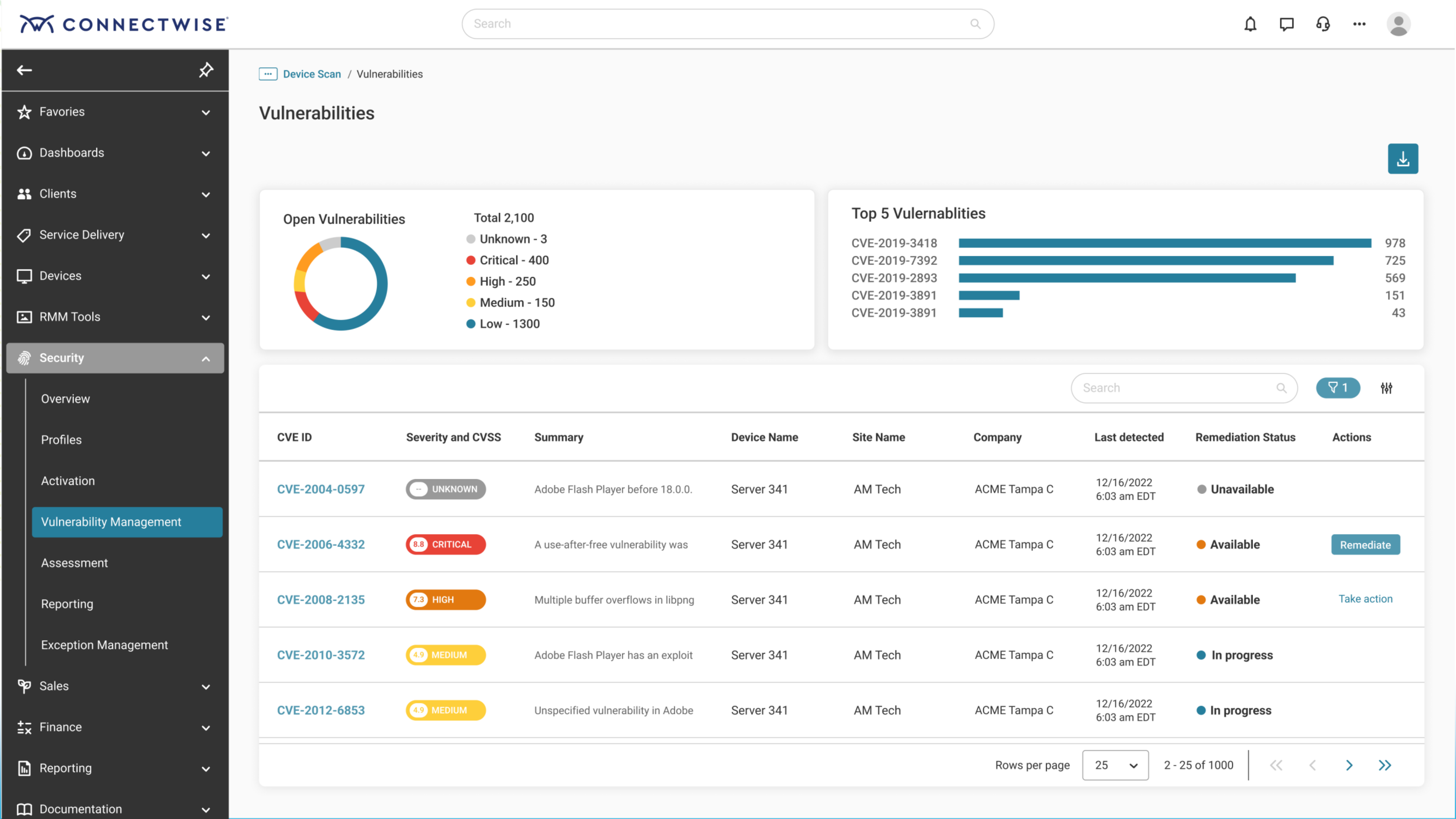
#ITNation

Questions ?

https://linktr.ee/cw.tcohn

Don't forget to fill out your

SESSION SURVEY



Vulnerabilities

Open Vulnerabilities

Total 2,100

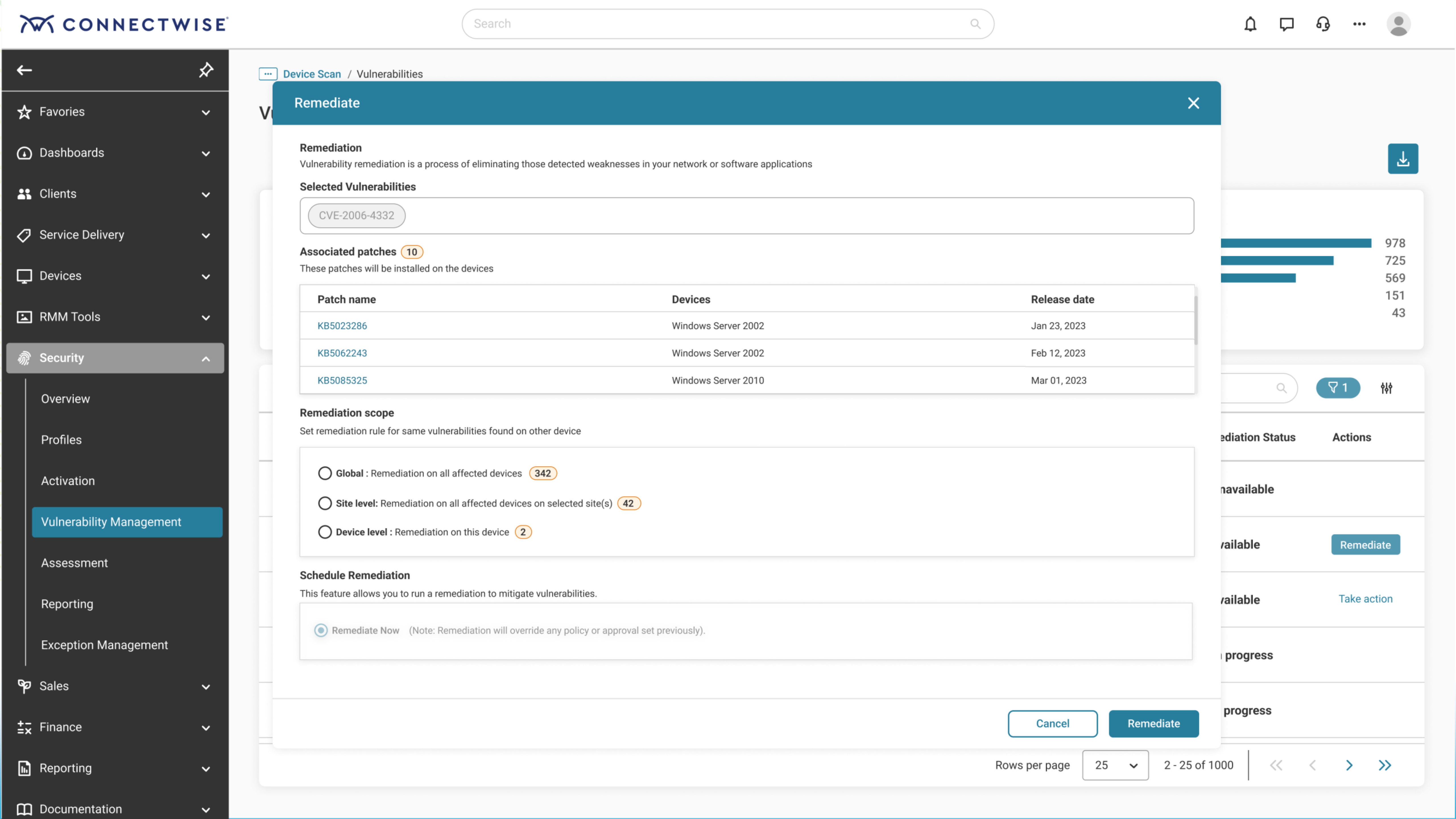
- ● Unknown - 3
- ● Critical - 400
- ● High - 250
- ● Medium - 150
- ● Low - 1300

Top 5 Vulnerablities

CVE-2019-3418	978
CVE-2019-7392	725
CVE-2019-2893	569
CVE-2019-3891	151
CVE-2019-3891	43

CVE ID	Severity and CVSS	Summary	Device Name	Site Name	Company	Last detected	Remediation Status	Actions
CVE-2004-0597	-- UNKNOWN	Adobe Flash Player before 18.0.0.	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Unavailable	
CVE-2006-4332	8.8 CRITICAL	A use-after-free vulnerability was	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Available	Remediate
CVE-2008-2135	7.3 HIGH	Multiple buffer overflows in libpng	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Available	Take action
CVE-2010-3572	4.9 MEDIUM	Adobe Flash Player has an exploit	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	
CVE-2012-6853	4.9 MEDIUM	Unspecified vulnerability in Adobe	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	

Rows per page 25 2 - 25 of 1000



Remediate

Remediation

Vulnerability remediation is a process of eliminating those detected weaknesses in your network or software applications

Selected Vulnerabilities

CVE-2006-4332

Associated patches 10

These patches will be installed on the devices

Patch name	Devices	Release date
KB5023286	Windows Server 2002	Jan 23, 2023
KB5062243	Windows Server 2002	Feb 12, 2023
KB5085325	Windows Server 2010	Mar 01, 2023

Remediation scope

Set remediation rule for same vulnerabilities found on other device

○ **Global** : Remediation on all affected devices 342

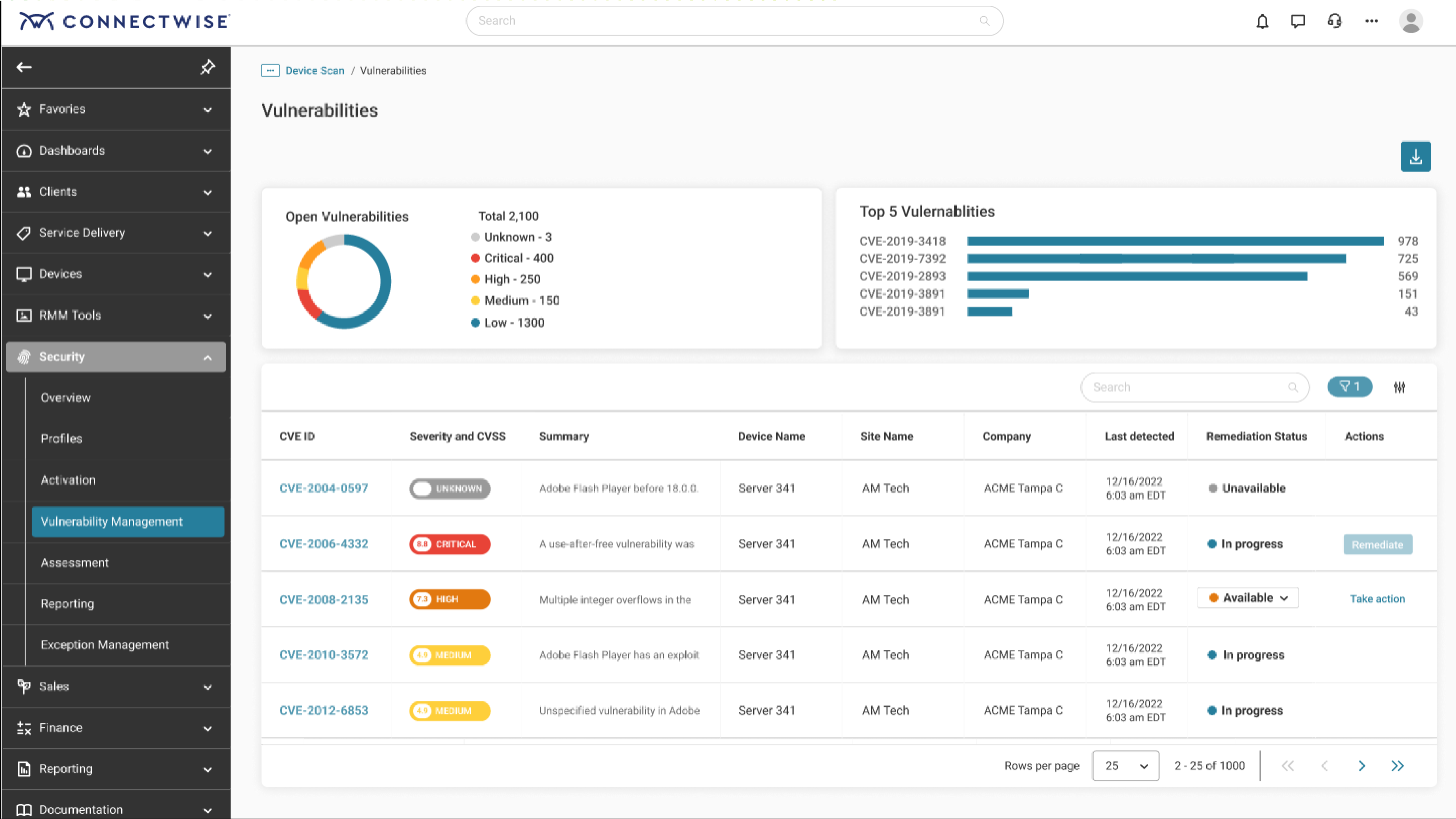
○ **Site level:** Remediation on all affected devices on selected site(s) 42

○ **Device level :** Remediation on this device 2

Schedule Remediation

This feature allows you to run a remediation to mitigate vulnerabilities.

● Remediate Now (Note: Remediation will override any policy or approval set previously).



Device Scan / Vulnerabilities

Vulnerabilities

Open Vulnerabilities

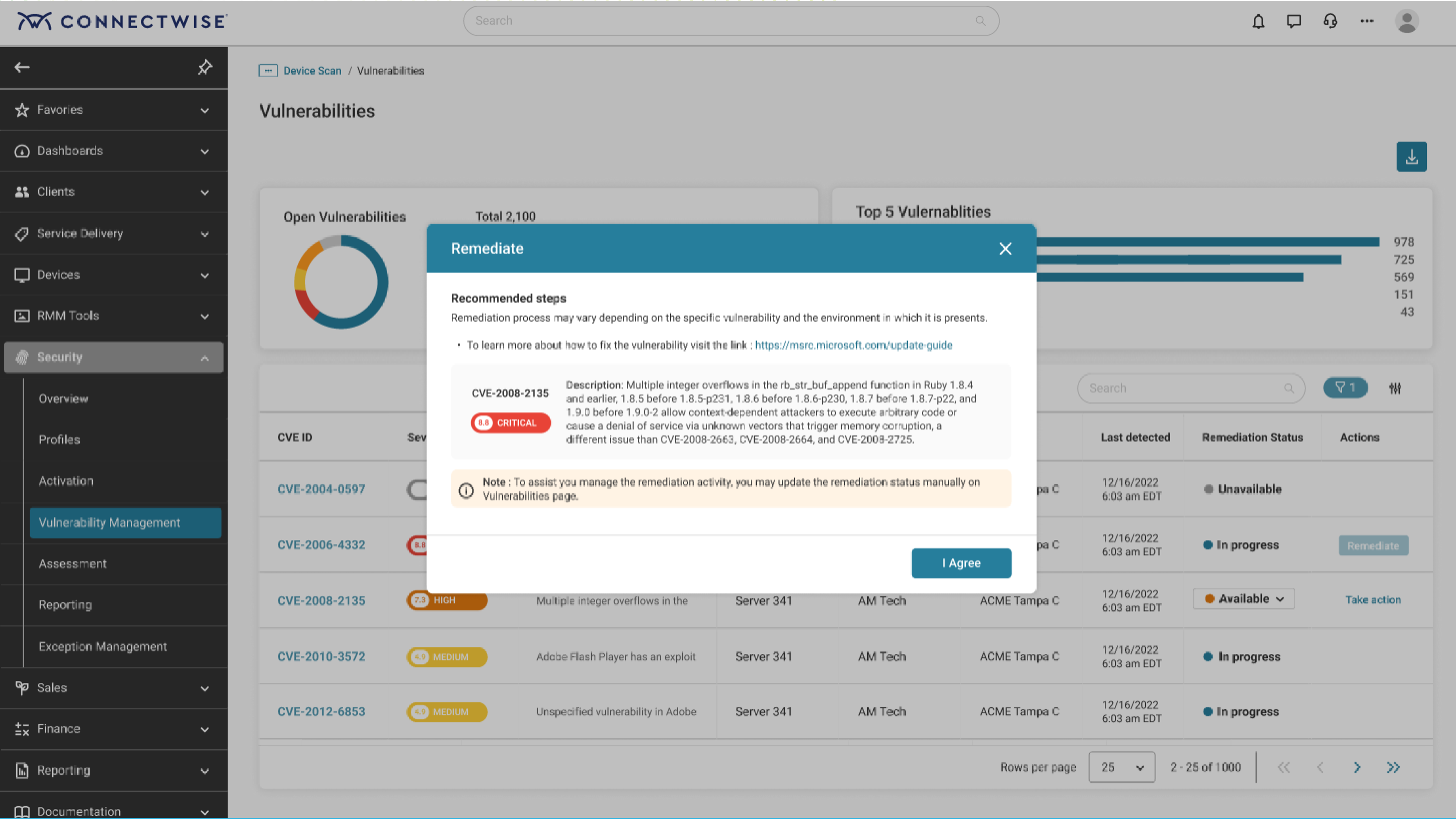
Total 2,100
- ● Unknown - 3
- ● Critical - 400
- ● High - 250
- ● Medium - 150
- ● Low - 1300

Top 5 Vulernablities

CVE-2019-3418	978
CVE-2019-7392	725
CVE-2019-2893	569
CVE-2019-3891	151
CVE-2019-3891	43

CVE ID	Severity and CVSS	Summary	Device Name	Site Name	Company	Last detected	Remediation Status	Actions
CVE-2004-0597	UNKNOWN	Adobe Flash Player before 18.0.0.	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Unavailable	
CVE-2006-4332	8.8 CRITICAL	A use-after-free vulnerability was	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	Remediate
CVE-2008-2135	7.3 HIGH	Multiple integer overflows in the	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Available	Take action
CVE-2010-3572	4.9 MEDIUM	Adobe Flash Player has an exploit	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	
CVE-2012-6853	4.9 MEDIUM	Unspecified vulnerability in Adobe	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	

Rows per page 25   2 - 25 of 1000



Remediate

Recommended steps

Remediation process may vary depending on the specific vulnerability and the environment in which it is presents.

- To learn more about how to fix the vulnerability visit the link : https://msrc.microsoft.com/update-guide

CVE-2008-2135

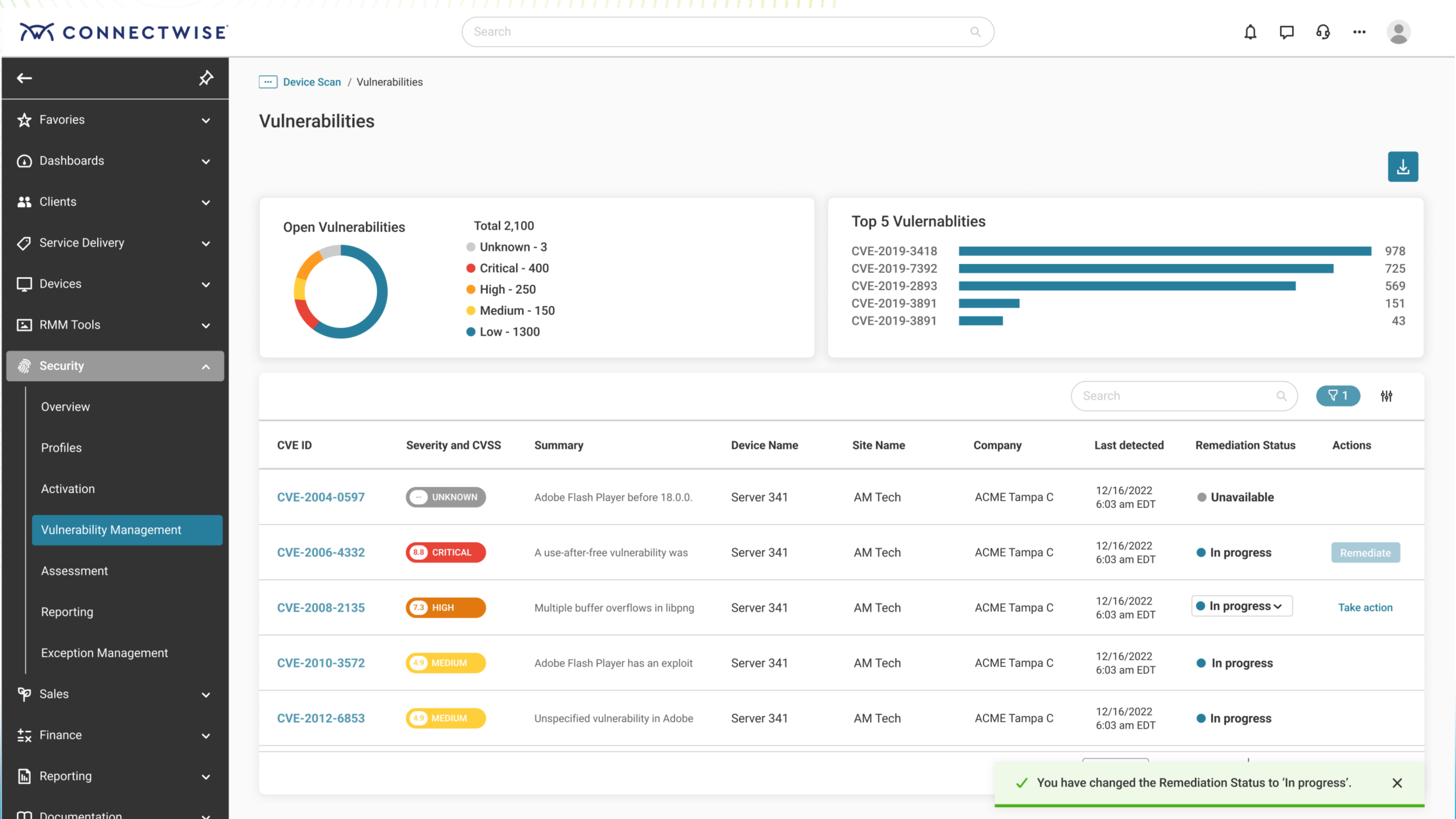
8.8 CRITICAL

Description: Multiple integer overflows in the rb_str_buf_append function in Ruby 1.8.4 and earlier, 1.8.5 before 1.8.5-p231, 1.8.6 before 1.8.6-p230, 1.8.7 before 1.8.7-p22, and 1.9.0 before 1.9.0-2 allow context-dependent attackers to execute arbitrary code or cause a denial of service via unknown vectors that trigger memory corruption, a different issue than CVE-2008-2663, CVE-2008-2664, and CVE-2008-2725.

Note : To assist you manage the remediation activity, you may update the remediation status manually on Vulnerabilities page.

CVE ID	Sev					Last detected	Remediation Status	Actions
CVE-2004-0597					pa C	12/16/2022 6:03 am EDT	● Unavailable	
CVE-2006-4332	8.8				pa C	12/16/2022 6:03 am EDT	● In progress	Remediate
CVE-2008-2135	7.3 HIGH	Multiple integer overflows in the	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Available	Take action
CVE-2010-3572	4.9 MEDIUM	Adobe Flash Player has an exploit	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	
CVE-2012-6853	4.9 MEDIUM	Unspecified vulnerability in Adobe	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	

Rows per page 25 2 - 25 of 1000



CONNECTWISE

Search

- Favories
- Dashboards
- Clients
- Service Delivery
- Devices
- RMM Tools
- Security
  - Overview
  - Profiles
  - Activation
  - Vulnerability Management
  - Assessment
  - Reporting
  - Exception Management
- Sales
- Finance
- Reporting
- Documentation

Device Scan / Vulnerabilities

Vulnerabilities

Open Vulnerabilities

Total 2,100

- ● Unknown - 3
- ● Critical - 400
- ● High - 250
- ● Medium - 150
- ● Low - 1300

Top 5 Vulnerablities

CVE-2019-3418	978
CVE-2019-7392	725
CVE-2019-2893	569
CVE-2019-3891	151
CVE-2019-3891	43

Search

CVE ID	Severity and CVSS	Summary	Device Name	Site Name	Company	Last detected	Remediation Status	Actions
CVE-2004-0597	-- UNKNOWN	Adobe Flash Player before 18.0.0.	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● Unavailable	
CVE-2006-4332	8.8 CRITICAL	A use-after-free vulnerability was	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	Remediate
CVE-2008-2135	7.3 HIGH	Multiple buffer overflows in libpng	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	Take action
CVE-2010-3572	4.9 MEDIUM	Adobe Flash Player has an exploit	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	
CVE-2012-6853	4.9 MEDIUM	Unspecified vulnerability in Adobe	Server 341	AM Tech	ACME Tampa C	12/16/2022 6:03 am EDT	● In progress	

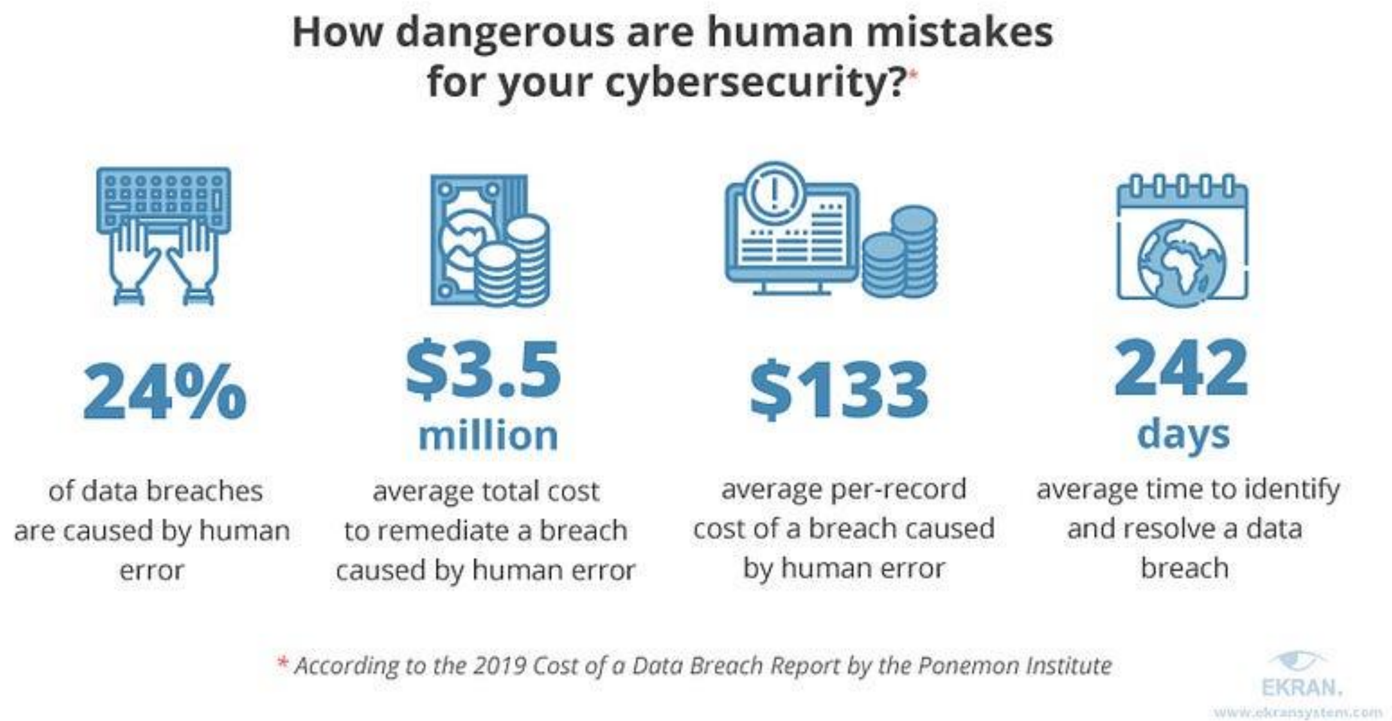
✓ You have changed the Remediation Status to 'In progress'.

Vulnerability Management in Numbers

95%

of Breaches are Caused by Human Error

Vulnerability Management in Numbers



How dangerous are human mistakes for your cybersecurity?*

24%

of data breaches are caused by human error

$3.5 million

average total cost to remediate a breach caused by human error

$133

average per-record cost of a breach caused by human error

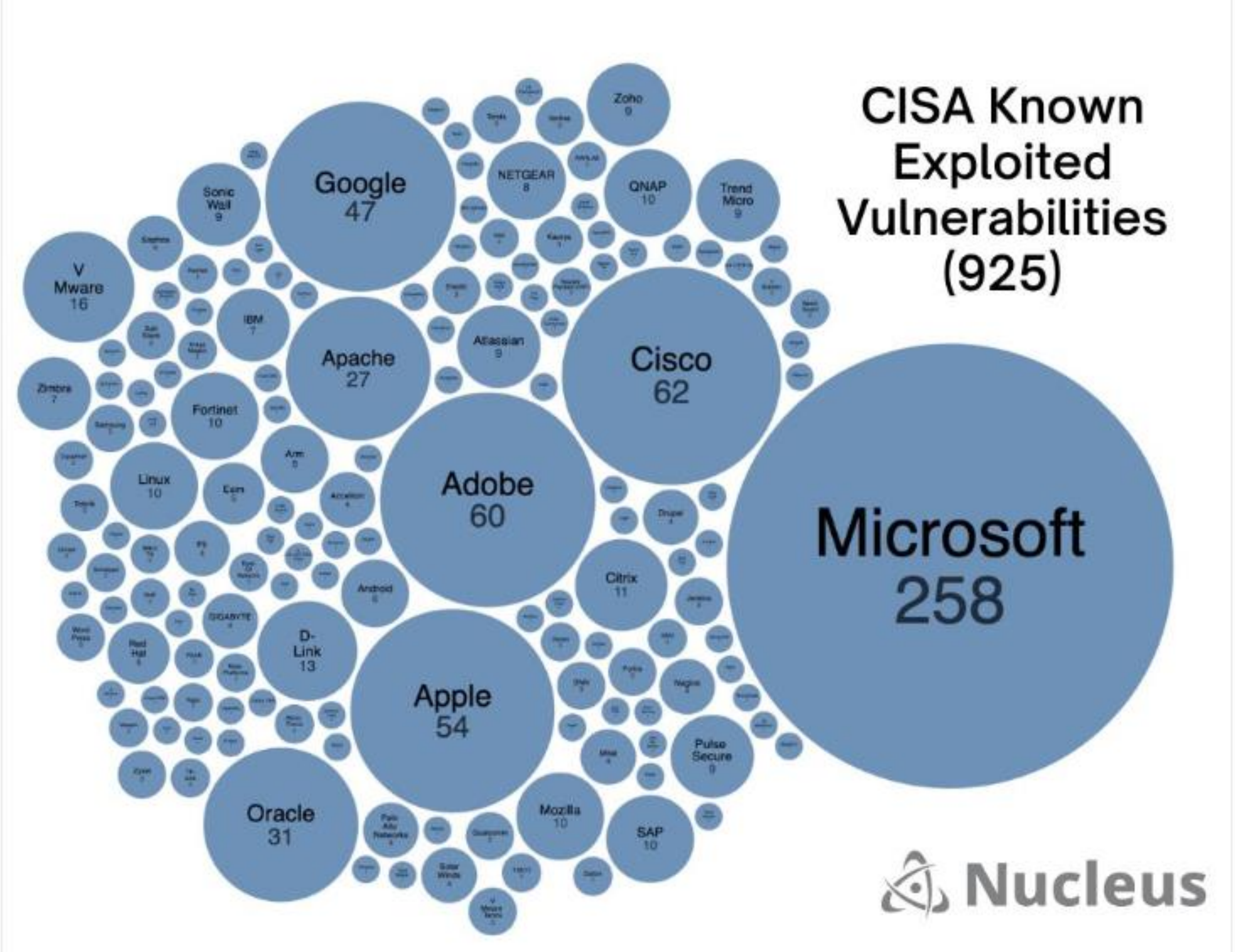
242 days

average time to identify and resolve a data breach

* *According to the 2019 Cost of a Data Breach Report by the Ponemon Institute*

EKRAN.
www.ekransystem.com

Vulnerability Management in Numbers

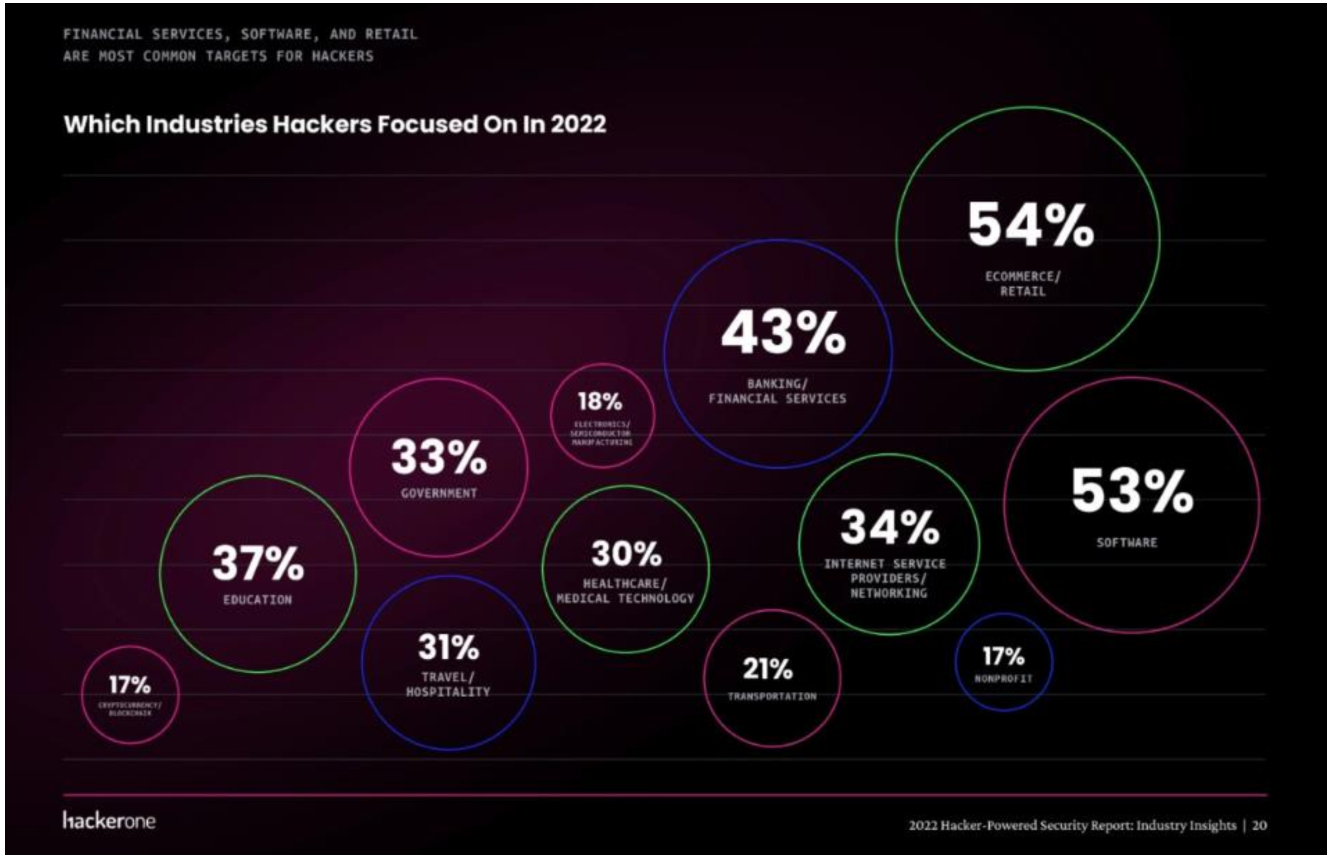


CISA Known Exploited Vulnerabilities (925)

#ITNation

https://www.linkedin.com/company/nucleussec

Vulnerability Management in Numbers



FINANCIAL SERVICES, SOFTWARE, AND RETAIL
ARE MOST COMMON TARGETS FOR HACKERS

Which Industries Hackers Focused On In 2022

hackerone

2022 Hacker-Powered Security Report: Industry Insights | 20

#ITNation

https://www.traceable.ai/blog-post/hackerone-2022-hacker-powered-security-report

IT NATION