

VERSATILITY

# Security and Trust Center

Connect. Secure. Simplify.

**Sunil Ravi**

CISO

VERSATILITY

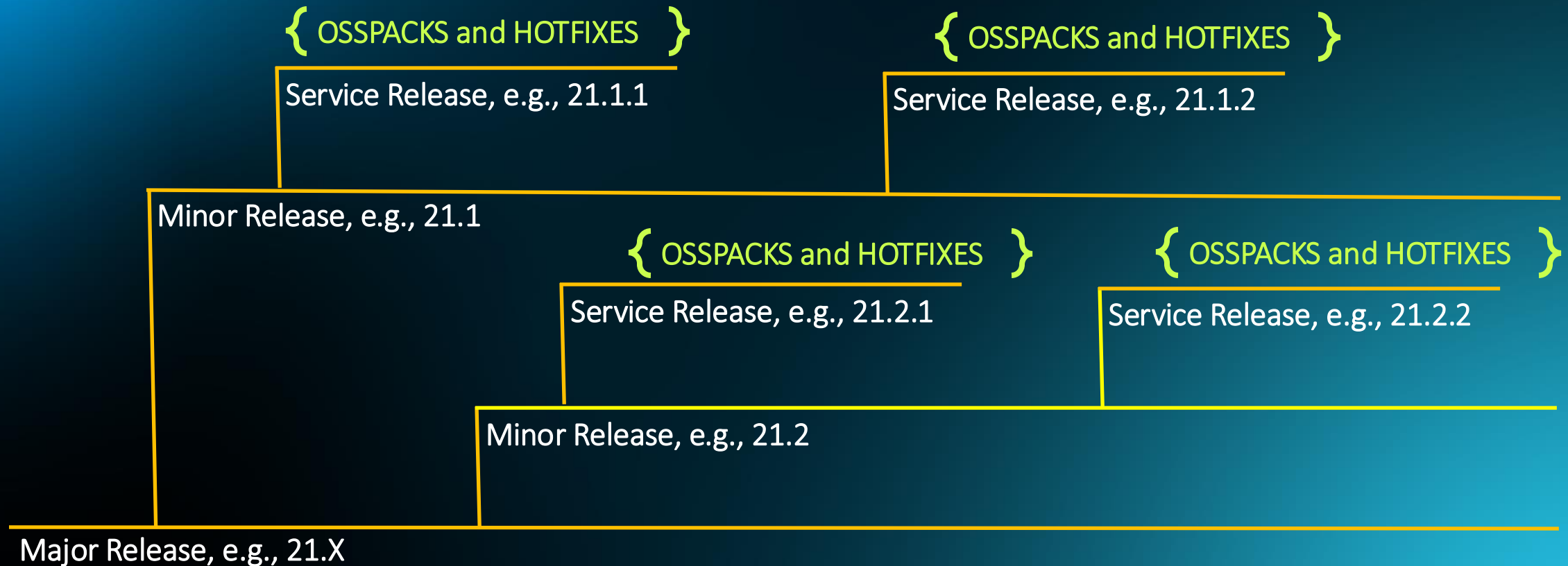
# Agenda

- PSIRT
  - Versa Software Releases
  - Kernel / OS Security
  - Application Security
  - Security Portal

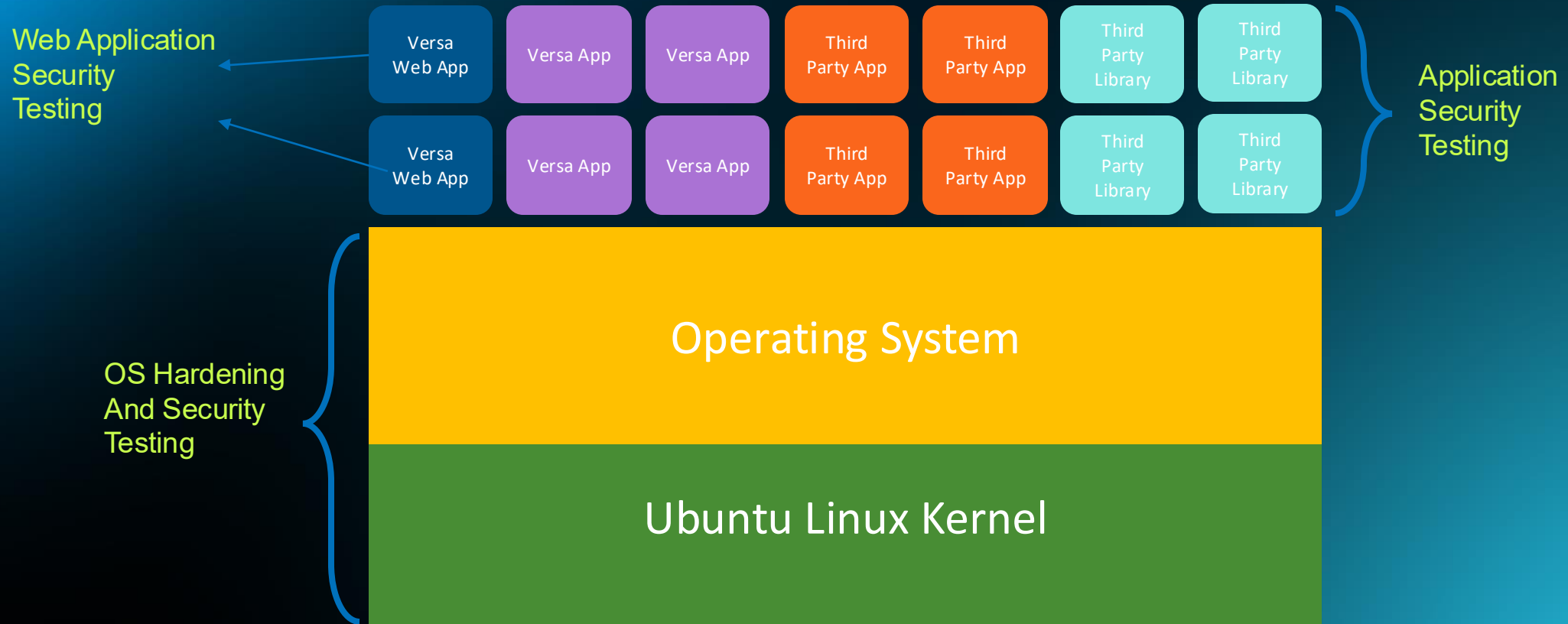
# Versa Software Releases

Product	Versions
Versa Director	21.1.4, 21.2.3, 21.3.3, 22.1.2, 22.1.3, 22.1.4, 22.1.5, 23.1.1
Versa Analytics	21.1.4, 21.2.3, 21.3.3, 22.1.2, 22.1.3, 22.1.4, 22.1.5, 23.1.1
VOS	21.1.4, 21.2.3, 21.3.3, 22.1.2, 22.1.3, 22.1.4, 22.1.5, 23.1.1
Versa Concerto	11.4.4, 12.2.2
Versa Messaging Server	5.2.2
Versa SASE Client	Windows: 7.9.5, MacOS: 7.7.1

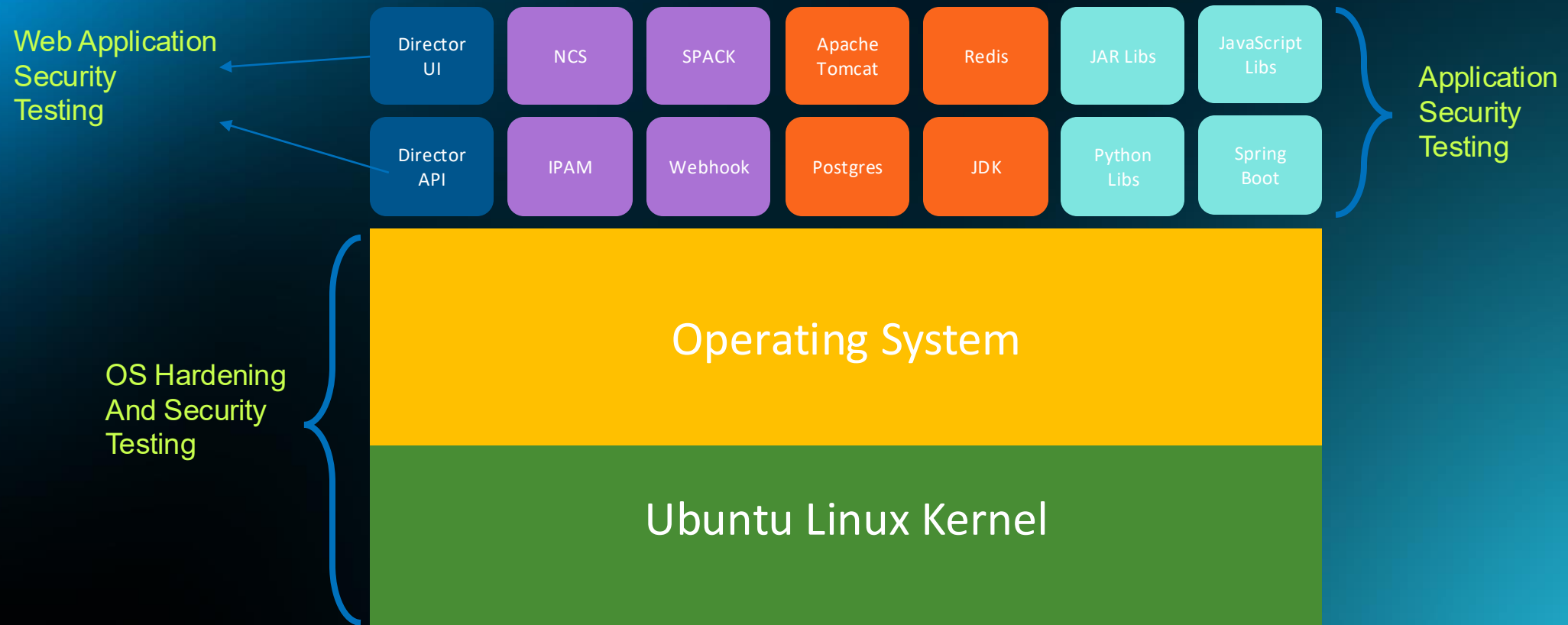
# Versa Software Patches



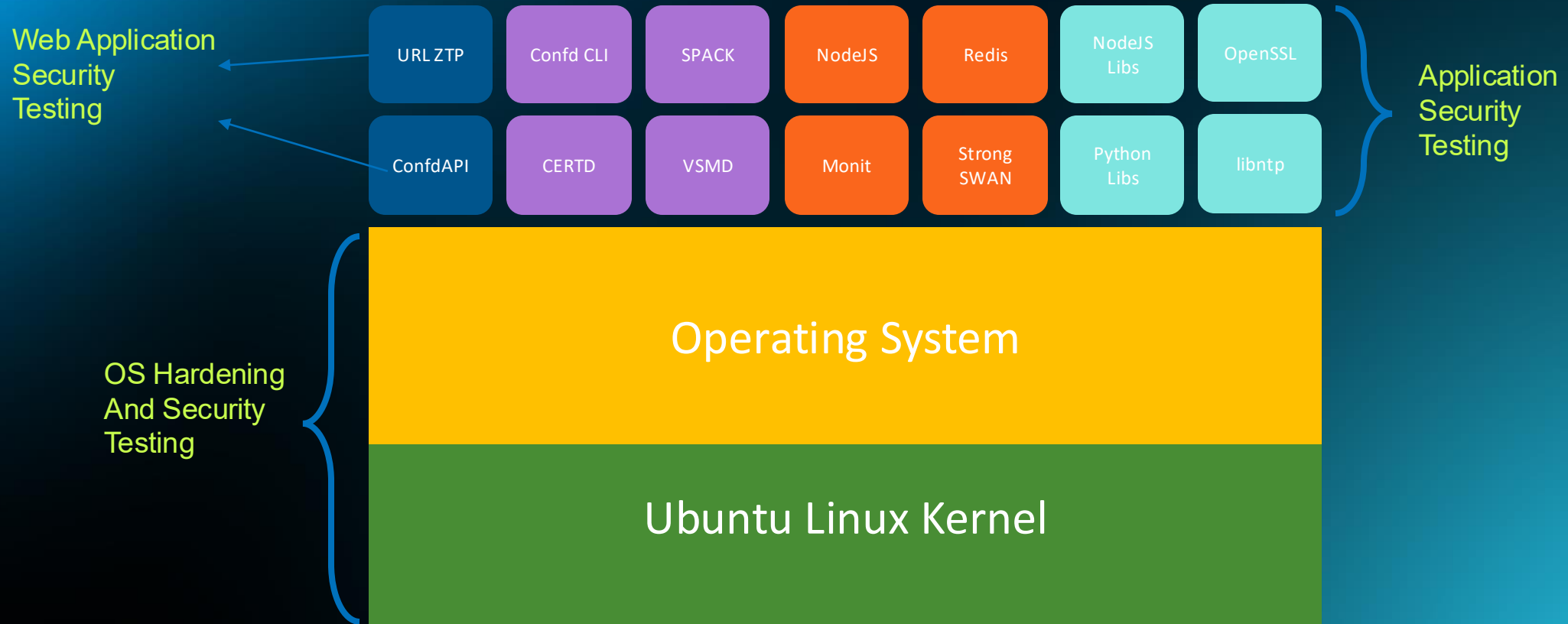
# Versa Software Stack



# Versa Software Stack - Director



# Versa Software Stack - VOS



# Static Analysis Security Testing (SAST)

- Nessus / Qualys / Orca
- Qualys Policy Compliance
- Grype
- Dependency Check
- Reversing Labs Spectra Assure
- Coverity
- SBOM

# Dynamic Analysis Security Testing (SAST)

- Internal Testing
  - Burp Suite
  - OWASP ZAP
  - Horizon3.ai
- Customer
- External
- Bug-Bounty

# OS Security

## OS Hardening

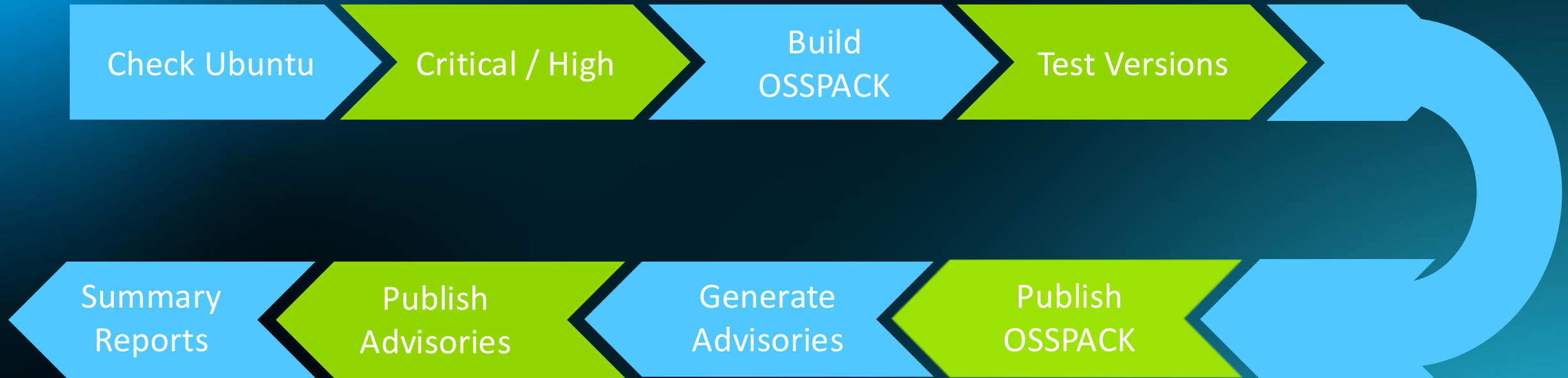
- Nessus Vulnerability Scan
- Qualys Vulnerability Scan
- Orca Vulnerability Scan
- Qualys CIS Profile
- Nmap

## Patch Management

- OSSPACKS for OS Security Updates
- Manual / Automatic Patching

- OS Security Hardening compliant to NIST/CIS Benchmarks
- Ensure no known Critical/High vulnerabilities at time of Versa software releases, including OSSPACKS and Hot Fixes
- Security patches to remediate vulnerabilities between Versa software releases
- No network/service downtime provides ability to apply Automatic OS Security Updates

# OS Security



# Kernel / Application Security

## Security Testing

- Several Fortune-500 companies and Service Providers
- Manual / Automated Pen Testing (Internal)
- Manual Pen Testing by NCC Group (External)
- Bug Bounty

## Testing Tools

- Dependency Check
- Orca
- Grype
- Coverity
- Reversing Labs Spectra Assure
- OWASP ZAP
- Burp Suite
- Horizon3.ai

- Applications tested with industry-standard SAST and DAST tools and methodologies
- Ensure no Critical/High severity vulnerabilities at time of software releases
- Application Security Updates delivered via Hot Fixes to remediate vulnerabilities between software releases
- Scheduled maintenance window for Service-impacting Kernel / Application Security Updates delivered via Hot Fix releases

# Kernel / Application Security

Nessus / Qualys / Orca

Grype / Dependency Check

Reversing Labs / SBOM

Coverity

Fixed

New – Fix Available

New – Fix Not Available

Rolled Over

Deploy Build

Initiate Scan

Export Reports

Classify / Prioritize

Summary Reports

Publish Advisories

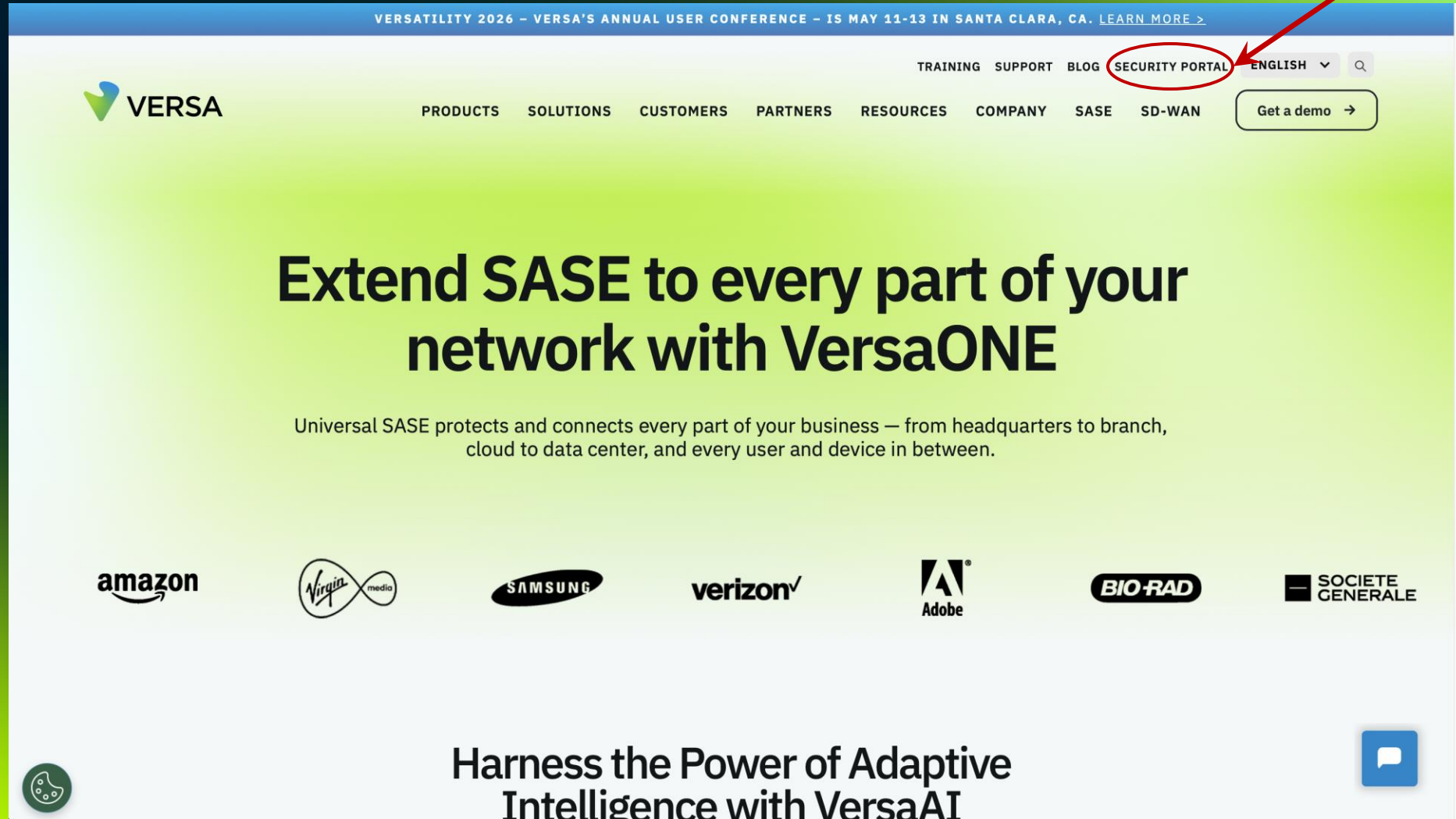
Generate Advisories

Create / Update Bugs

# Versa Vulnerability Policy

Vulnerability Type	Patch Cadence	Emergency Patches	Notification	Patch Mechanism
Kernel	90 days	1-7 days	Monthly	Hot Fixes
OS	1-3 days (Critical / High)	1-7 days	1–3 days	OSSPACK
Application	30 days 90 days in case of disruptive upgrades	1-7 days	Monthly	Hot FIXes

# Security Portal for PSIRT



VERSATILITY 2026 – VERSA'S ANNUAL USER CONFERENCE – IS MAY 11-13 IN SANTA CLARA, CA. [LEARN MORE >](#)



TRAINING SUPPORT BLOG **SECURITY PORTAL** ENGLISH



VERSIA

PRODUCTS SOLUTIONS CUSTOMERS PARTNERS RESOURCES COMPANY SASE SD-WAN [Get a demo →](#)

## Extend SASE to every part of your network with VersaONE


Universal SASE protects and connects every part of your business – from headquarters to branch, cloud to data center, and every user and device in between.


amazon  SAMSUNG verizon  BIO-RAD SOCIETE GENERALE

 Harness the Power of Adaptive Intelligence with VersaAI 

# Security Portal for PSIRT

VERSATILITY 2026 – VERSA'S ANNUAL USER CONFERENCE – IS MAY 11-13 IN SANTA CLARA, CA. LEARN MORE >

TRAINING SUPPORT BLOG SECURITY PORTAL ENGLISH 

 PRODUCTS SOLUTIONS CUSTOMERS PARTNERS RESOURCES COMPANY SASE SD-WAN [Get a demo →](#)

## Versa Security and Trust Center


Stay informed with valuable insights into today's threat environment, including significant vulnerabilities, important cybersecurity news, trending threat actors, and solutions to defend your network against cyberattacks.


### Versa Security Portal

Access to Versa's PSIRT advisories, Threat Library, and public advisories.

[Log in →](#) [Public Advisories →](#)

THREAT INTELLIGENCE SECURITY COMPLIANCE AND CERTIFICATION

 [FEATURED THREAT INTELLIGENCE REPORT](#)

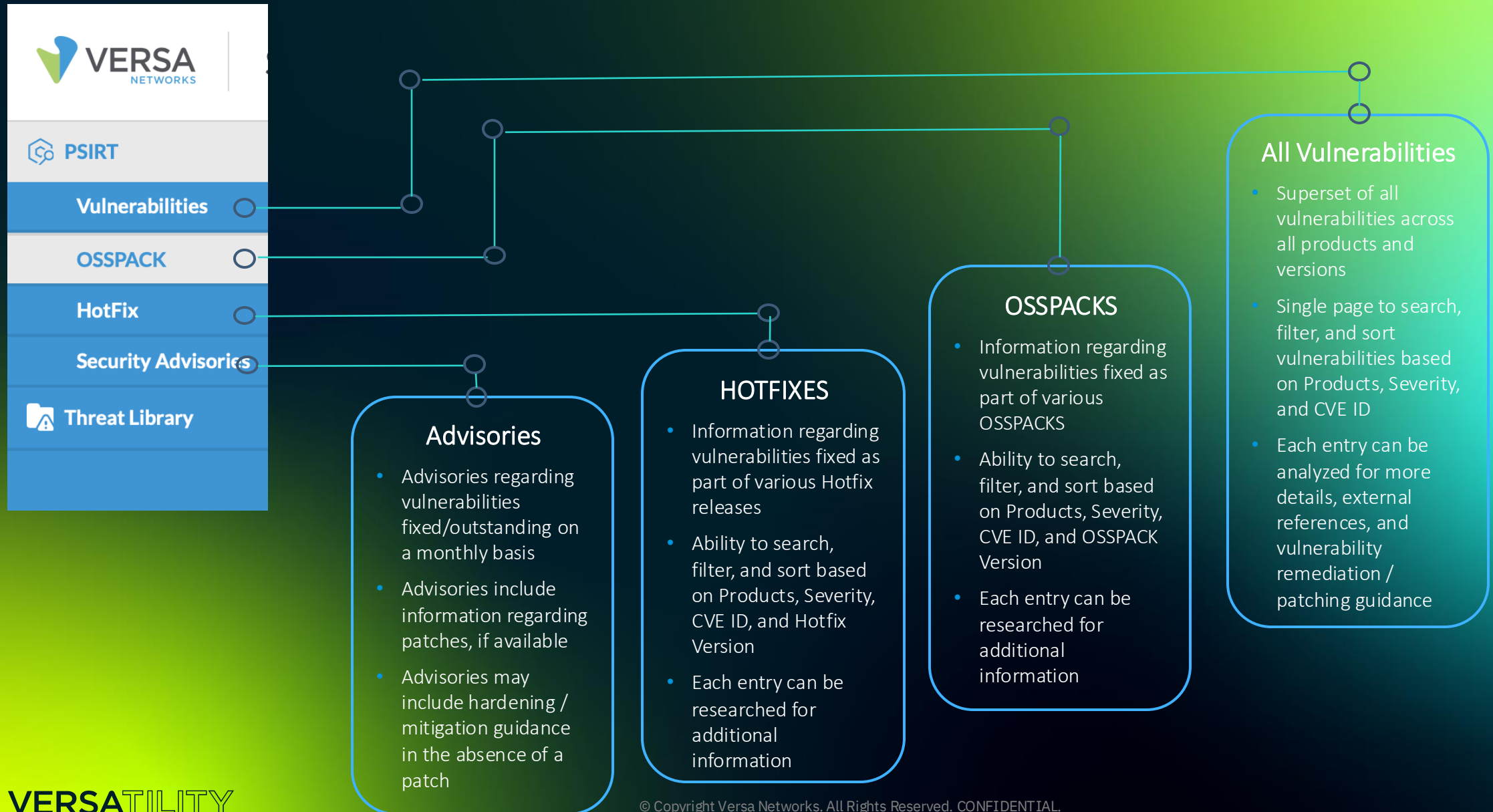
[VERSAS CYBER – THREAT INTELLIGENCE REPORTS](#) 

# Security Portal for PSIRT

The Versa Product Security Incident Response Team (PSIRT) issues advisories on issues in Versa products, accompanied by their resolutions or other recommendations. PSIRT is a dedicated team that handles the investigation, analysis, resolution, and disclosure of vulnerabilities and issues in Versa products. Advisories are released as part of Operating System Security Package (OSSPACK) updates and other updates that are specific to Versa products and their components.

CVE ID ↑ ↓	Summary	Product ▼	Severity	Date Published	Date Updated ▼	Affected Versions ▼	Fixed Version
▶ CVE-2025-26465	A vulnerability was found...	Analytics	Medium	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 21...	OSSPACK 20250224
▶ CVE-2025-26465	A vulnerability was found...	Concerto	Medium	Feb 18, 2025	---	11.2.2, 11.2.3, 10.2.1, 11...	OSSPACK 20250224
▶ CVE-2025-26465	A vulnerability was found...	Director	Medium	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 22...	OSSPACK 20250224
▶ CVE-2025-26465	A vulnerability was found...	VOS	Medium	Feb 18, 2025	---	20.2.4, 21.1.4, 21.1.3, 21...	OSSPACK 20250224
▶ CVE-2024-56171	libxml2 before 2.12.10 an...	Analytics	High	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 21...	OSSPACK 20250303
▶ CVE-2025-27113	libxml2 before 2.12.10 an...	Analytics	Low	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 21...	OSSPACK 20250303
▶ CVE-2025-24928	libxml2 before 2.12.10 an...	Analytics	High	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 21...	OSSPACK 20250303
▶ CVE-2024-56171	libxml2 before 2.12.10 an...	Concerto	High	Feb 18, 2025	---	11.2.2, 11.2.3, 10.2.1, 11...	OSSPACK 20250303
▶ CVE-2025-27113	libxml2 before 2.12.10 an...	Concerto	Low	Feb 18, 2025	---	11.2.2, 11.2.3, 10.2.1, 11...	OSSPACK 20250303
▶ CVE-2025-24928	libxml2 before 2.12.10 an...	Concerto	High	Feb 18, 2025	---	11.2.2, 11.2.3, 10.2.1, 11...	OSSPACK 20250303
▶ CVE-2024-56171	libxml2 before 2.12.10 an...	Director	High	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 22...	OSSPACK 20250303
▶ CVE-2025-27113	libxml2 before 2.12.10 an...	Director	Low	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 22...	OSSPACK 20250303
▶ CVE-2025-24928	libxml2 before 2.12.10 an...	Director	High	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 22...	OSSPACK 20250303
▶ CVE-2024-56171	libxml2 before 2.12.10 an...	VOS	High	Feb 18, 2025	---	20.2.4, 21.1.4, 21.1.3, 21...	OSSPACK 20250303

# Security Portal for PSIRT



# Security Portal for PSIRT

- Click [Follow](#) button on top-right of each page to automatically get notified when there are content updates on that page
- Click [Unfollow](#) button on top-right of each page to unsubscribe from the notifications

**VERSA NETWORKS** Security Portal

PSIRT

Sort Severity Select Product Select Sort CVE ID's Select

Follow

The Versa Product Security Incident Response Team (PSIRT) issues advisories on issues in Versa products, accompanied by their resolutions or other recommendations. PSIRT is a dedicated team that handles the investigation, analysis, resolution, and disclosure of vulnerabilities and issues in Versa products. Advisories are released as part of Operating System Security Package (OSSPACK) updates and other updates that are specific to Versa products and their components.

CVE ID ↑ ↓	Summary	Product ▼	Severity	Date Published	Date Updated ▼	Affected Versions ▼	Fixed Version
▶ CVE-2025-26465	A vulnerability was found...	Analytics	Medium	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 21...	OSSPACK 20250224
▶ CVE-2025-26465	A vulnerability was found...	Concerto	Medium	Feb 18, 2025	---	11.2.2, 11.2.3, 10.2.1, 11...	OSSPACK 20250224
▶ CVE-2025-26465	A vulnerability was found...	Director	Medium	Feb 18, 2025	---	20.2.2, 20.2.3, 20.2.4, 22...	OSSPACK 20250224
▶ CVE-2025-26465	A vulnerability was found...	VOS	Medium	Feb 18, 2025	---	20.2.4, 21.1.4, 21.1.3, 21...	OSSPACK 20250224

# Security Portal for PSIRT

The screenshot displays the 'Security Portal' interface for PSIRT. The top navigation bar includes the 'VERSA NETWORKS' logo and the text 'Security Portal'. On the right side of the header, there are icons for a notification bell with the number '27' and a user profile icon. A left-hand sidebar contains three menu items: 'PSIRT', 'Security Library', and 'Vulnerability Form', with 'Vulnerability Form' currently selected. The main content area is titled 'Security Vulnerability Form List' and features a prominent 'Security Vulnerability Report' heading. Below this heading is a sub-header: 'Help us keep our products secure by reporting potential vulnerabilities'. The form is organized into several sections: 1. 'Reporter Information' section, which includes input fields for 'Full Name \*' (placeholder: 'Your full name'), 'Email Address \*' (placeholder: 'your.email@example.com'), and 'Company/Organization \*' (placeholder: 'Your organization'). 2. 'Vulnerability Details' section, which contains four dropdown menus: 'Vulnerability Type \*' (placeholder: 'Select Type'), 'Affected Product/Service \*' (placeholder: 'Select Product'), 'Severity Level \*' (placeholder: 'Select severity'), and 'Product Version' (placeholder: 'e.g., 1.0.0'). 3. 'Detailed Description \*' section, a large text area with the placeholder text 'Provide a comprehensive description of the vulnerability, including technical details...'. 4. 'Steps to Reproduce \*' section, a text area with the placeholder text '1. Step one', '2. Step two', and '3. Step three...'. 5. 'Impact Assessment \*' section, a text area with the placeholder text 'What could an attacker achieve? What data/systems are at risk?'. The form uses a clean, modern design with blue accents and red asterisks to denote required fields.

VERSATILITY

Thank You!