NIST & Cisco CVE/PSIRT integrations

Associate Cisco PSIRT advisories and NIST/NVD CVE information with discovered devices and software.

The business requirement

Vulnerability lists become useful when they are connected to the devices and software the team operates. Device Manager integrates Cisco support information and the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). Common Vulnerabilities and Exposures (CVE) records and Cisco Product Security Incident Response Team (PSIRT) advisories give engineers a starting point for assessment and response.



HOW THE CAPABILITY WORKS

Establish device and software context

Discover the fleet and maintain device hardware and software information in Device Manager. Advisory matching depends on this context and the supported integration.

Enable the advisory integrations

Gluware uses API integration with NIST/NVD for multi-vendor CVE information and Cisco Support API integration for Cisco PSIRT advisories, including their CVEs. Cisco CVE information comes from Cisco, not NIST/NVD.

Review and prioritize the findings

Inspect device-associated advisories alongside inventory. Use the available records and reports to scope investigation and planned maintenance. Advisory information is not, by itself, confirmation that the live device is exposed.

Connect intelligence to action

Use Titan Exposure Analysis for contextual assessment with OS, configuration, and operational state. Supported remediation can use OS Manager or Config Model Editor through the appropriate governed execution path.

NIST & Cisco CVE/PSIRT integrations

Connect the operating process to defined component responsibilities.

COMPONENTS DELIVERING THE CAPABILITY

Device Manager	Owns Cisco Support API and NIST/NVD integrations and device-associated advisory data.
Gluware Control	Supplies integration configuration, credentials, and access controls.
Titan Exposure Analysis	Adds contextual CVE relevance assessment without making changes.
OS Manager	Performs supported software deployment when an update is selected.
Config Model Editor	Performs modeled CLI/API configuration changes when a compensating control is selected.

OPERATING SCOPE

Device Manager: advisory source ownership

Gluware uses API integration with NIST/NVD for multi-vendor CVE information and Cisco Support API integration for Cisco PSIRT advisories, including their CVEs. Cisco CVE information comes from Cisco, not NIST/NVD. Cisco Support API also provides EoL/EoS and SmartNet status.

Titan Exposure Analysis: contextual assessment

Assess vulnerabilities against discovered OS information, configuration, and operational state rather than relying on the version alone.

Titan Exposure Remediation: supported response

The remediation component of Titan Exposure Management can orchestrate supported patches or compensating controls with approvals, validation, and outcome verification.

> **Business value and measurement**
>
> Measure advisory coverage, devices awaiting assessment, and time from a relevant finding to verified action. Device Manager owns the advisory integration and display; Titan Exposure Analysis adds the separate contextual assessment.

Technical documentation | Request a demo

Current integration support