DATA SHEET

Supply chain vulnerabilities

What to know after the curl and libcurl hype

Why are software supply chain vulnerabilities a risk?

Defending against software supply chain vulnerabilities is of utmost importance when it comes to safeguarding the integrity and security of software systems. In light of recent events, such as the disclosure of two vulnerabilities in the widely used command line tool and library, curl, it has become evident that vulnerabilities in the software supply chain pose a significant risk. These vulnerabilities, categorized as high and low severities by most vendors, have the potential to impact a wide range of applications due to their inclusion in the SBOMs (Software Bill of Materials) of popular software programs.

Software supply chain vulnerabilities refer to the weaknesses or risks associated with a software product, particularly those that arise from the utilization of third-party libraries and components. For instance, if a widely used open-source library like "curl" and "libcurl" is found to have a vulnerability, it can render multiple dependent applications susceptible to attacks. This becomes even more concerning when considering that over 90% of commercial codebases incorporate open-source software (OSS) components, such as "curl" and "libcurl," which are often critical to the functioning of various applications and parts of an organization's IT ecosystem.

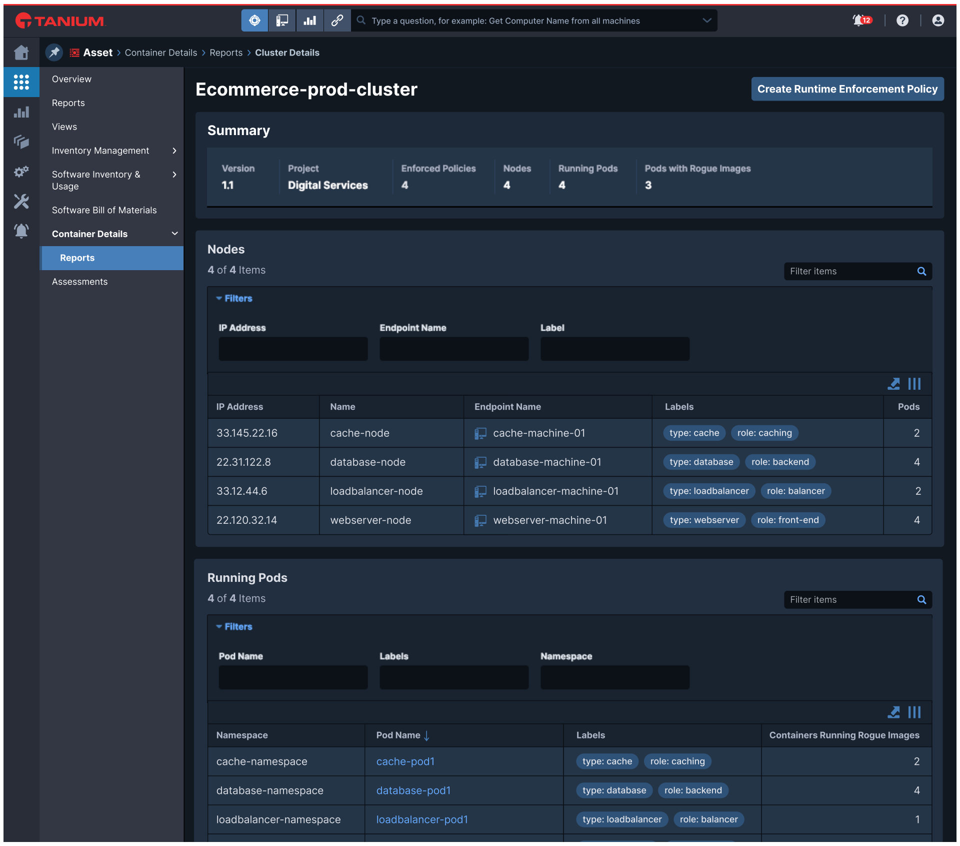
The escalating prevalence of software supply chain attacks, with a staggering 742% increase year over year since 2019, as reported in the "State of the Software Supply Chain," highlights the urgent need for organizations to proactively monitor and update their software components, including open-source libraries, in order to mitigate these vulnerabilities. By implementing robust security practices, such as conducting regular vulnerability assessments and efficient patch management, organizations can minimize the potential impact of supply chain vulnerabilities on their IT ecosystem.

How Tanium can help

As a solution, Tanium offers a comprehensive range of measures to help organizations defend against future vulnerabilities in the software supply chain. From proactive monitoring and identification of vulnerable components to timely patching and updates, Tanium provides the necessary tools and expertise to ensure the security and integrity of software systems.

Eliminate blind spots:

OSS and libraries such as "curl" and "libcurl" are source code that software vendors need to compile into their codebase to provide specialized functions. Initially, they are statically integrated into the program, but once implemented and deployed, they become dynamically linked resources. Traditional vulnerability scanners struggle to detect these compiled libraries, making them difficult or even impossible to find. Therefore, a solution like Tanium is needed to scan and identify OSS components/ libraries during runtime. Tanium allows you to easily identify all runtime libraries, open-source freeware, and software packages with just a click of a button.


TANIUM
Type a question, for example: Get Computer Name from all machines
12
Asset › Container Details › Reports › Cluster Details
Overview
Reports
Views
Inventory Management
Software Inventory & Usage
Software Bill of Materials
Container Details
Reports
Assessments
Create Runtime Enforcement Policy
Filter items
Filters

Ecommerce-prod-cluster

Summary

Version	Project	Enforced Policies	Nodes	Running Pods	Pods with Rogue Images
1.1	Digital Services	4	4	4	3

Nodes

4 of 4 Items

IP Address / Endpoint Name / Label

IP Address	Name	Endpoint Name	Labels	Pods
33.145.22.16	cache-node	cache-machine-01	type: cache role: caching	2
22.31.122.8	database-node	database-machine-01	type: database role: backend	4
33.12.44.6	loadbalancer-node	loadbalancer-machine-01	type: loadbalancer role: balancer	2
22.120.32.14	webserver-node	webserver-machine-01	type: webserver role: front-end	4

Running Pods

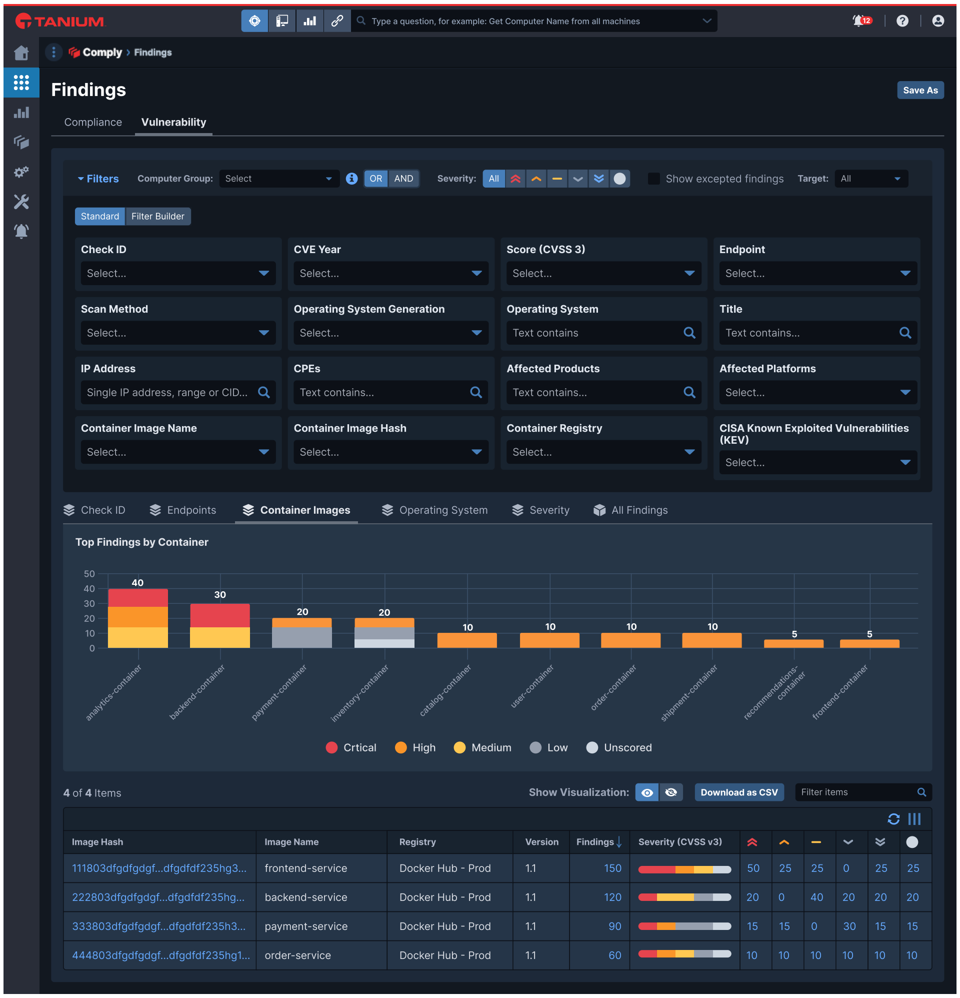
4 of 4 Items

Pod Name / Labels / Namespace

Namespace	Pod Name ↓	Labels	Containers Running Rogue Images
cache-namespace	cache-pod1	type: cache role: caching	2
database-namespace	database-pod1	type: database role: backend	4
loadbalancer-namespace	loadbalancer-pod1	type: loadbalancer role: balancer	1

Prioritize:

Certain systems and endpoints are more crucial to business operations and may require immediate attention if found to be vulnerable. This is particularly important if the vulnerability is highly likely to be exploited, considering factors such as the presence of public exploits, ongoing campaigns by threat actors, or the system's high value or internet-facing position. With the visibility provided by Tanium, you can prioritize which applications, systems, and endpoints to address first.



Findings

Computer Group: Select · Severity: All · ☐ Show excepted findings · Target: All

Check ID	CVE Year	Score (CVSS 3)	Endpoint
Select...	Select...	Select...	Select...

Scan Method	Operating System Generation	Operating System	Title
Select...	Select...	Text contains	Text contains...

IP Address	CPEs	Affected Products	Affected Platforms
Single IP address, range or CID...	Text contains...	Text contains...	Select...

Container Image Name	Container Image Hash	Container Registry	CISA Known Exploited Vulnerabilities (KEV)
Select...	Select...	Select...	Select...

4 of 4 Items

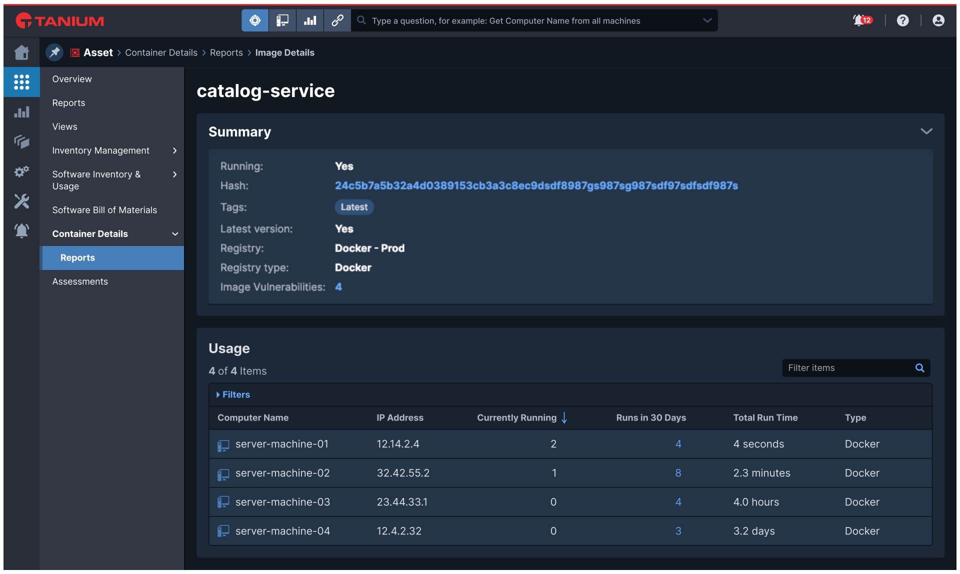
Image Hash	Image Name	Registry	Version	Findings ↓	Severity (CVSS v3)	︽	︿	—	﹀	︾	●
111803dfgdfgdgf...dfgdfdf235hg3...	frontend-service	Docker Hub - Prod	1.1	150		50	25	25	0	25	25
222803dfgdfgdgf...dfgdfdf235hg...	backend-service	Docker Hub - Prod	1.1	120		20	0	40	20	20	20
333803dfgdfgdgf...dfgdfdf235h3...	payment-service	Docker Hub - Prod	1.1	90		15	15	0	30	15	15
444803dfgdfgdgf...dfgdfdf235hg1...	order-service	Docker Hub - Prod	1.1	60		10	10	10	10	10	10

Get your personalized demo to see first-hand how Tanium SBOM can secure your software supply chain.

See Tanium in action

ALREADY A TANIUM CLIENT?

Contact your Tanium representative to learn about adding Tanium SBOM to your platform.


TANIUM
Type a question, for example: Get Computer Name from all machines
12
Asset › Container Details › Reports › Image Details
Overview
Reports
Views
Inventory Management
Software Inventory & Usage
Software Bill of Materials
Container Details
Reports
Assessments
Filter items
Filters

catalog-service

Summary

Running: Yes
Hash: 24c5b7a5b32a4d0389153cb3a3c8ec9dsdf8987gs987sg987sdf97sdfsdf987s
Tags: Latest
Latest version: Yes
Registry: Docker - Prod
Registry type: Docker
Image Vulnerabilities: 4

Usage

4 of 4 Items

Computer Name	IP Address	Currently Running ↓	Runs in 30 Days	Total Run Time	Type
server-machine-01	12.14.2.4	2	4	4 seconds	Docker
server-machine-02	32.42.55.2	1	8	2.3 minutes	Docker
server-machine-03	23.44.33.1	0	4	4.0 hours	Docker
server-machine-04	12.4.2.32	0	3	3.2 days	Docker

Take action:

Now that you understand the vulnerability and its location within your environment, you can proceed with remediation. Tanium offers various options for taking action:

- Push out patches to all devices
- Strengthen system security through configuration management
- Control and manage user access
- Whitelist or blacklist applications
- Terminate relevant processes
- Isolate devices from the environment
- Remove affected apps completely from endpoints

What you need:

Adding defense against supply chain vulnerabilities is made easy with Tanium. The Tanium solution offers a single package that allows you to find and identify vulnerabilities that are hidden within the SBOMs (Software Bill of Materials) of applications across all your endpoints. This protection is included in our Core Tier X2. For companies with fewer than 10K endpoints, we offer our Emerging Enterprise Professional Tier, which provides the same protection.

For existing customers who have purchased Tanium Asset, all you will need is Tanium SBOM.

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. Visit us at www.tanium.com.