BACKBOX

SOLUTION BRIEF

Closed-loop Vulnerability Remediation with BackBox

Using dynamic inventory with risk data and scoring to help administrators prioritize and perform device OS updates with the greatest impact on network security.

Overview

As cyber-attacks leveraging unpatched devices become a common practice, an effort-saving comprehensive network security management platform is a must, empowering businesses to proactively identify vulnerabilities and strengthen their defenses against cyber threats.

> “**Through 2026, more than 60% of threat detection, investigation and response (TDIR) capabilities will leverage exposure management data to validate and prioritize detected threats, up from less than 5% today.”** Gartner 12/22

This presents a challenge for network and security device administrators.

Vulnerability patching for endpoints and compute systems is easier than patching network and security devices. Updating devices like firewalls, IDSs, IPSs, routers, switches, and WAPs to patch CVEs is much more complicated, as each device impacts the entire network operations and security infrastructure. The BackBox network cyber resilience platform, working together with vulnerability intelligence can optimize the work invested in OS Updates in a way that maximizes the security impact on the network.

NIST lists over 2,500 CVEs per month. That's a lot of "out-of-context security information" for network administrators to consume. CVEs also serve, in part, as a roadmap for attackers to target network vulnerabilities. It's important to understand how CVEs pertain to your specific network inventory, taking the risk to your organization from the abstract to the specific.

The challenge is that permanently addressing the vulnerabilities disclosed in the CVEs requires an OS update or patch to the network devices. These updates are often complicated and time consuming, requiring after-hours work, sometimes with impacting the business.

This results in OS updates and vulnerability patches being delayed and deprioritized even though "unpatched software is a top three access route for hackers, and patching remains the most important thing you can do to secure your technology." [1]

Fortunately, there's now a better way for network operations teams and service providers of all sizes to protect networks while reducing the intensity of manual work these software updates entail.

[1] https://thestack.technology/analysis-of-cves-in-2022-software-vulnerabilities-cwes-most-dangerous/

CLOSED-LOOP VULNERABILITY REMEDIATION

- **Dynamic Inventory.** With BackBox, there's no guessing about your inventory. You want to ensure you have a complete and current view of your network and security devices. Collecting inventory information is an error-prone, manual process completed as part of provisioning new devices or updating existing ones. With BackBox, collecting your inventory is simple and automatic, and you can trust that the inventory information passed into a vulnerability risk scoring engine is complete and accurate.

- **Risk Scoring and Analytics.** BackBox vulnerability intelligence risk scoring engine reviews vulnerabilities impacting the organization and provides attack surface score and risk metrics for every connected device on the network. It understands and presents contextual risk across all devices and networks for a complete view of network vulnerabilities and risk exposure. The risk score integrates CVSS scores along with the number of CVEs on the device, whether or not a CVE is under active exploit, and if the device being scored is internet-facing.

- **CVE Mitigation.** Administrators can search device configuration files for specific vulnerable configurations to determine the relevance of any given CVE. If a vulnerability is found, using automation, it can be mitigated, and once mitigated, it's removed from the risk score. However, some CVEs will be determined to be irrelevant to the device. In that case, administrators can make the CVE non-applicable to the device, causing the risk score to recalculate and present an accurate view of the vulnerability state of the device. These non-applicable CVEs, called "mitigated" in the product, can be managed in their interface so that if they become relevant later in the future, they can be re-added.

- **Remediation Prioritized by Risk Analysis.** BackBox takes the complexity from the patching process while giving administrators risk analysis data to prioritize updates. This data helps create consensus and provides a complete picture of the priority of vulnerability patching, while the pre-built automations make deploying updates easier than ever before. Network Vulnerability Manager even provides insight into step upgrades, enabling organizations to easily understand how their security posture improves by updating, but not to the most recent version.

Most network engineers would agree that updating an OS for its own sake is an administrative exercise, but patching vulnerabilities is critical. Should CVEs expose vulnerabilities, there are important steps to take immediately, followed by the software update, which is a permanent fix.

Let's explore the process of vulnerability patching in a little more detail.

Without BackBox

There are five elements to patching vulnerabilities:

1. Understand your inventory and exposures
2. Determine the update priorities
3. Remediate with temporary configuration fixes
4. Remediate permanently with OS updates
5. Remove temporary configuration fixes

We hear from many of our customers that this end-to-end update cycle is manual. Even when inventory is kept in a central system, there's a lack of confidence that it is complete and up-to-date for an important task like vulnerability patching due to shortcomings in the discovery process.

Similarly, the inventory system is not a "working system." Inventory needs to be exported somewhere (like a spreadsheet or database) to verify and perhaps manipulate it, for example, ordering vulnerability patches by priority relative to business need. Additionally, once the inventory is out of the inventory system, it should be assumed to be out of date with any adds, moves, or changes that occur after the export.

Once visibility into inventory is available, a similar exercise needs to happen with CVEs.

CVEs, if they're tracked at all, are tracked manually in a spreadsheet or a database, with some limited ordering based on priority and associated with the equipment in the inventory. Additional information can be correlated manually from other sources to enrich that presented in the CVE. It's a lot of manual effort.

This can result in ambiguity and blind spots. For example, how does my security posture improve if I update to a newer version, but not the latest, a common practice? Or, of the critical vulnerabilities my network is exposed to, which ones are currently being exploited in the wild? You might prioritize those vulnerabilities with known exploits if that exploit information were presented in the context of the rest of the security scoring.

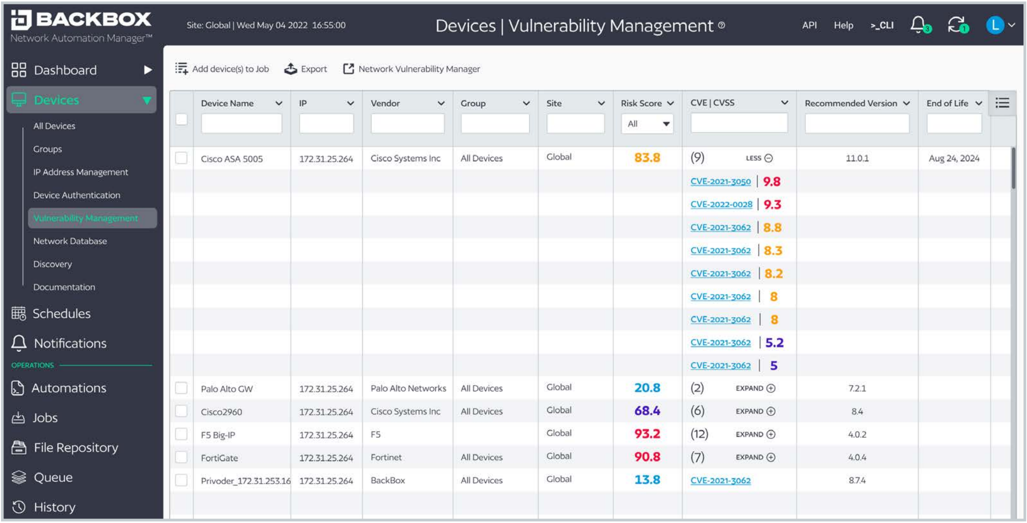
Temporary configuration changes are easy enough to make with the usual processes at the organization, but software updates remain highly disruptive. Additionally, temporary configuration changes have a nasty habit of becoming permanent simply due to a lack of systems to track which devices have been temporarily patched and then updated.

Lacking a security score and hard data on the impact of potential protection updates, they're moved to after-hours administrative work driven by a vague notion that being on the latest version is better. And, without automation closing the loop between inventory and the vulnerability patch, the effort is time consuming, error-prone, and leaves a big time gap between known vulnerability and patched vulnerability that can be maliciously exploited.

With BackBox Vulnerability Intelligence

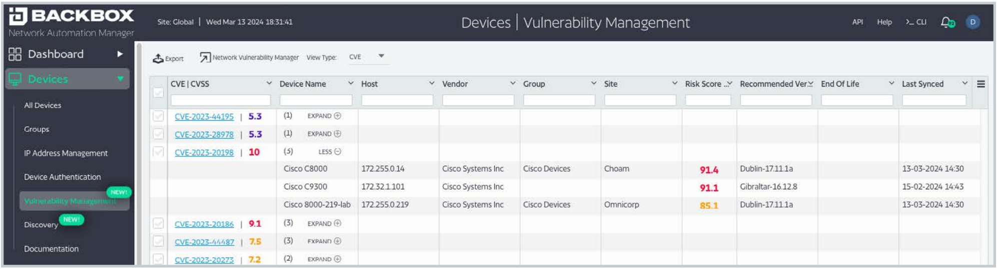
BackBox has closed the loop between dynamic inventory and OS update prioritization by integrating a continuously updating operational security database of CVE information, risk scoring, and other security metadata. This provides several key benefits:

- Devices are discovered through an automated process. Once discovered, an inventory is collected which is used later in the flow to map against vulnerabilities and CVEs.
- After the initial discovery and inventory, administrators continue to gain daily inventory information directly from the network itself through discovery automation rather than having to depend on manually tracking adds, moves, and changes. Having a daily inventory means that information about the network is always current.
- Administrators use risk and vulnerability scoring to prioritize OS updates and configuration changes that help protect the organization.



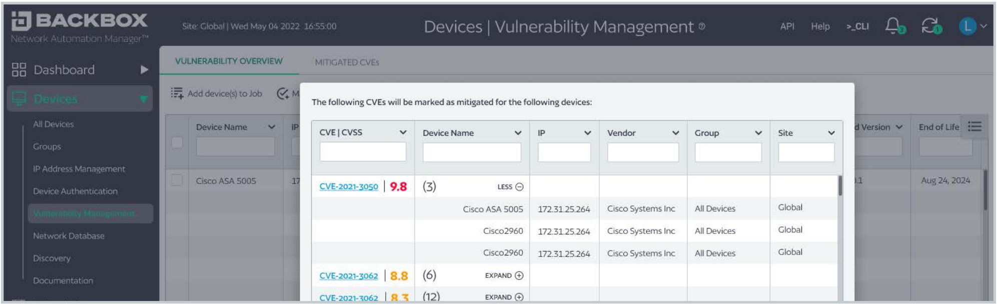
Device Name	IP	Vendor	Group	Site	Risk Score	CVE | CVSS		Recommended Version	End of Life
					All				
Cisco ASA 5005	172.31.25.264	Cisco Systems Inc	All Devices	Global	83.8	(9)	LESS ⊖	11.0.1	Aug 24, 2024
						CVE-2021-3050 | 9.8			
						CVE-2022-0028 | 9.3			
						CVE-2021-3062 | 8.8			
						CVE-2021-3062 | 8.3			
						CVE-2021-3062 | 8.2			
						CVE-2021-3062 | 8			
						CVE-2021-3062 | 8			
						CVE-2021-3062 | 5.2			
						CVE-2021-3062 | 5			
Palo Alto GW	172.31.25.264	Palo Alto Networks	All Devices	Global	20.8	(2)	EXPAND ⊕	7.2.1	
Cisco2960	172.31.25.264	Cisco Systems Inc	All Devices	Global	68.4	(6)	EXPAND ⊕	8.4	
F5 Big-IP	172.31.25.264	F5		Global	93.2	(12)	EXPAND ⊕	4.0.2	
FortiGate	172.31.25.264	Fortinet	All Devices	Global	90.8	(7)	EXPAND ⊕	4.0.4	
Privoder_172.31.253.16	172.31.25.264	BackBox	All Devices	Global	13.8	CVE-2021-3062		8.7.4	

- Administrators can also view their vulnerabilities by CVE to make it easier to manage a particular vulnerability that they know requires attention.



CVE | CVSS	Device Name	Host	Vendor	Group	Site	Risk Score	Recommended Ver	End Of Life	Last Synced
CVE-2023-44195 | 5.3	(1) EXPAND ⊕								
CVE-2023-28978 | 5.3	(1) EXPAND ⊕								
CVE-2023-20198 | 10	(5) LESS ⊖								
	Cisco C8000	172.255.0.14	Cisco Systems Inc	Cisco Devices	Choam	91.4	Dublin-17.11.1a		13-03-2024 14:30
	Cisco C9300	172.32.1.101	Cisco Systems Inc			91.1	Gibraltar-16.12.8		15-02-2024 14:43
	Cisco 8000-219-lab	172.255.0.219	Cisco Systems Inc	Cisco Devices	Omnicorp	85.1	Dublin-17.11.1a		13-03-2024 14:30
CVE-2023-20186 | 9.1	(3) EXPAND ⊕								
CVE-2023-44487 | 7.5	(3) EXPAND ⊕								
CVE-2023-20273 | 7.2	(2) EXPAND ⊕								

- Sometimes, CVEs are determined to be irrelevant to a particular device (or group of devices). In the CVE detail, administrators can search through device configurations to look for the configuration elements being exploited. If they're not present, these CVEs can be marked 'mitigated' so they are removed from the risk scoring, giving network teams a more accurate view on their vulnerability state. CVEs can be marked 'mitigated' pre-device basis allowing for a lot of flexibility in how vulnerabilities are managed.

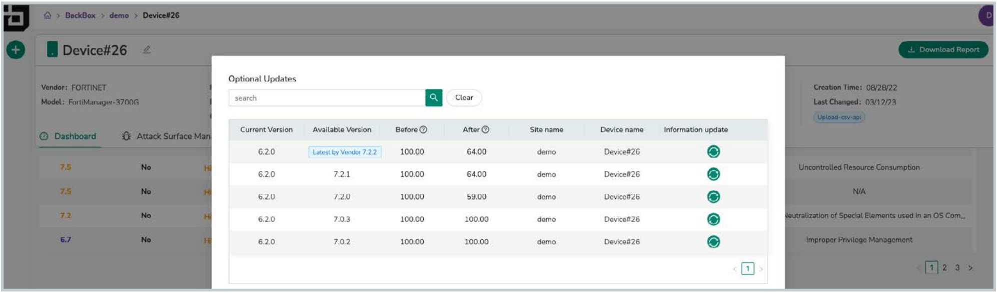


The following CVEs will be marked as mitigated for the following devices:

CVE | CVSS	Device Name	IP	Vendor	Group	Site
CVE-2021-3050 | 9.8	(3) LESS ⊖				
	Cisco ASA 5005	172.31.25.264	Cisco Systems Inc	All Devices	Global
	Cisco2960	172.31.25.264	Cisco Systems Inc	All Devices	Global
	Cisco2960	172.31.25.264	Cisco Systems Inc	All Devices	Global
CVE-2021-3062 | 8.8	(6) EXPAND ⊕				
CVE-2021-3062 | 8.3	(12) EXPAND ⊕				

- Like the network inventory, the CVE, vulnerability, and risk data that informs the analysis are also updated daily. The result is that both inventory and vulnerability/risk information is updated and correlated daily, giving administrators a current view of their network exposure to cyber threats.

- Administrators have a view on their specific environment so that if a latest release has a bug affecting their deployment, risk-adjusted scenarios can be examined to determine the optimal update path.


BackBox > demo > Device#26
D
Device#26
Download Report
Dashboard
Attack Surface Man
7.5
No
7.5
No
7.2
No
6.7
No
Uncontrolled Resource Consumption
N/A
Neutralization of Special Elements used in an OS Com...
Improper Privilege Management
1 2 3 >

Vendor: FORTINET
Model: FortiManager-3700G

Creation Time: 08/28/22
Last Changed: 03/12/23
Upload-csv-api

Optional Updates

search | Clear

Current Version	Available Version	Before	After	Site name	Device name	Information update
6.2.0	Latest by Vendor 7.2.2	100.00	64.00	demo	Device#26	●
6.2.0	7.2.1	100.00	64.00	demo	Device#26	●
6.2.0	7.2.0	100.00	59.00	demo	Device#26	●
6.2.0	7.0.3	100.00	100.00	demo	Device#26	●
6.2.0	7.0.2	100.00	100.00	demo	Device#26	●

- Administrators can update devices most efficiently, whether updates require multi-step updates or high-availability awareness.

Conclusion

> **[Vulnerability] patching remains the single most important thing you can do to secure your technology and is why applying patches is often described as 'doing the basics'."**[2] (UK National Cyber Security Center; Jul 10, 2019)

Vulnerability patching is hard. It's time-consuming, manual work often done after hours. While BackBox has always made it easier and faster to complete updates, they were still done without insight into vulnerability severity or the actual risk to the organization, until now.

With BackBox, networks can be kept more secure, with OS updates prioritized by risk and vulnerability data. Administrators can act on known inventory and be certain they have complete network visibility. Inventory is correlated with up-to-date data on CVEs and known risks, giving administrators a current view of their network exposure to the latest cyber threats. As always, updates are done in the most efficient way possible with support for over 180 vendors in the built-in Automation Library.

[2] https://www.ncsc.gov.uk/blog-post/the-problems-with-patching

About BackBox

More than 500 enterprises worldwide trust BackBox as their preferred network cyber resilience platform. BackBox supports network devices from over 180 vendors, offering thousands of pre-built automations and a no-code way to create new ones. BackBox empowers teams with the confidence to automate critical network processes, maintain business continuity during disruptions, and recover swiftly. From backups and OS updates to configuration compliance and vulnerability management, BackBox ensures that automations deliver consistent, reliable outcomes.

To learn more, visit **backbox.com**