



SECUREB4
We Strengthen Your Security

Secureb4.io

Importance Of Vulnerability Management

Contact us +971 565612349 | info@secureb4.io



Why Do We Need Vulnerability Management?



SECUREB4
We Strengthen Your Security



Identification of software
faults affecting security



Mitigating new security
risks



Foil automated attacks



Effective management of
security risks



Compliance with security
audit and regulations



Vulnerability Manager

- One of the most basic information security principles is identifying and managing vulnerabilities. With the passive scanning method, SecHard operates the vulnerability detection and management processes for all IT assets without creating any risks.
- SecHard collects information about assets and their software using the asset manager and device manager modules. SecHard can import scores generated by third-party vulnerability scanning tools and include them in the risk management process. At the same time, SecHard can send the information that it generated to third-party software.

Secureb4.io

Secureb4.io

Vulnerability Manager in SECHARD Tool

The screenshot shows the SECHARD tool's vulnerability management interface. At the top, there is a navigation bar with links for Dashboard, Security Zone, Management, Monitoring, Custom, Console, Assets, and a specific entry for 'F1 Switch - 172.16.0.12'. On the far right, there is a user icon labeled 'sechard'.

The main content area is titled 'Resource Vulnerability' and displays a 'Vulnerability (CVE) List'. A progress bar at the top indicates a score of 37%. Below the bar, there is a search and filter section with dropdowns for 'All', 'Exploited' (which is selected), and 'Not Exploited'. There are also filters for 'Search Date', 'Search Detection Date', 'Search Description', 'Search Severity', and a dropdown for '20'.

The main table lists vulnerabilities with columns for Vuln ID, Exploit, Published, SecHard Detection Date, Description, and CVSS Severity. The first row, CVE-2019-12655, is detailed below:

| Vuln ID | Exploit | Published | SecHard Detection Date | Description | CVSS Severity |
|----------------|---------|---------------------------------|---------------------------------|---|----------------------------------|
| CVE-2019-12655 | N/A | September 26, 2019; 00:15:00 AM | September 23, 2020; 13:52:29 PM | A vulnerability in the FTP application layer gateway (ALG) functionality used by Network Address Translation (NAT), NAT IPv6 to IPv4 (NAT64), and the Zone-Based Policy Firewall (ZBFW) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to a buffer overflow that occurs when an affected device inspects certain FTP traffic. An attacker could exploit this vulnerability by performing a specific FTP transfer through the device. A successful exploit could allow the attacker to cause the device to reload. | V3.1: 7.5 HIGH V2.0: 7.8 HIGH |

Other rows in the table include CVE-2010-3049, CVE-2010-3050, and CVE-2021-34705, each with their respective details.



Contact us +971 565612349 | info@secureb4.io

SECUREB4
We Strengthen Your Security

Benefits Of SECHard

Vulnerability Manager



SECUREB4
We Strengthen Your Security



Passive vulnerability scanning



Public exploit availability



CVSS based risk scoring



Detailed reports and alarms



Integration with third parties

Contact us

+971 565612349

info@secureb4.io



Summary

- As a hybrid solution, SecHard is able to perform all the NIST Cybersecurity Framework functions and the recommended processes of Gartner Adaptive Security Architecture without the need for experts.
- SecHard is a game-changer that complies with the Executive Office of the President Memorandum (M-22-09) and NIST SP 800-207 Zero Trust Architecture publication.
- Security analysis and remediation with SecHard are automated, which provides a significant return on investment (ROI) tens of times higher than other information security products.
- It is a fantastic technology that works agentless and requires no changes to your environment, and can be installed in an hour. It also supports bidirectional APIs for easy third-party integration.



Implement a Zero-Trust Security Model

The Unprecedented growth in ransomware attacks has shifted the reactive thinking of organizations & they are ready to embrace a security model that can accommodate a distributed workforce and remote work culture and give confidence in the security within their organization.

Secureb4.io

The zero-trust architecture and a centralized zero-trust platform are the need of the hour. SecureB4, in partnership with SecHard, brings you a complete suite of zero trust.

Contact us Now!

+971 565612349

info@secureb4.io



Secureb4.io

IS THIS CONTENT USEFUL?

-  If you found this post helpful, please like it
-  Share your thoughts in the comment section
-  Tell your friends about it
-  Save this post, in case you want to see it again