

SECURITY AS A SERVICE - VULNERABILITY IDENTIFICATION SERVICE (VIS)

Security is a critical concern for any institution connected to the Internet. DARKReading reported in 2018 that nearly 60% of the organizations that suffered a data breach in the past two years cite a not yet patched, known vulnerability as the root cause.*

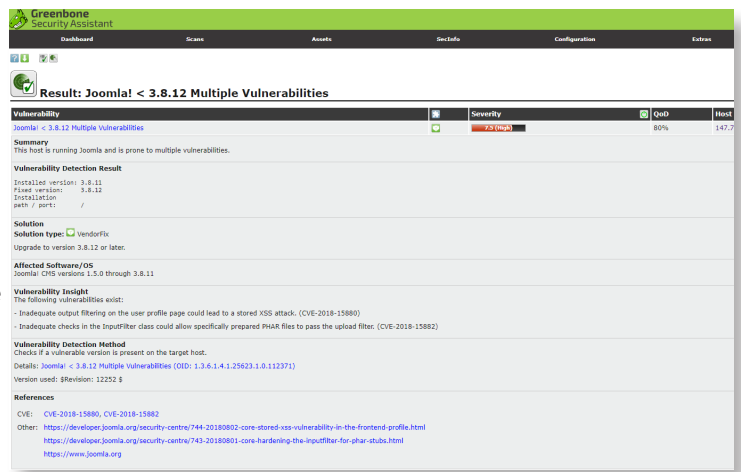
Many institutions do not have resources to do everything themselves. Three Rivers Optical Exchange (3ROX) offers a suite of services under its Security as a Service category that are designed to augment an institution's staff and help them prioritize activities to improve their security posture.

VIS Details

Three Rivers Optical Exchange (3ROX) offers a vulnerability identification service that will probe the IP address range of a campus for active machines and services, including the ones you don't know about. Network Vulnerability Tests (NVTs) are run against active machines/services to detect misconfigurations and known defects. A report is generated and sent to the member that lists any issue found by severity and host, allowing campus IT personnel to prioritize remediation. Each issue includes a list of vendor and/or community recommended fixes or corrective actions.

These scans are performed on a regular schedule and can be supplemented with on-demand scans. This flexibility provides regular assessments of exposed vulnerabilities and allows IT personnel to scan a new server or service for vulnerabilities shortly after it is made available.

**Approximately 37% of the breached organization admitted they don't scan for vulnerabilities.*



Result: Joomla! < 3.8.12 Multiple Vulnerabilities

Vulnerability	Severity	QoD	Host
Joomla! < 3.8.12 Multiple Vulnerabilities	High	80%	147.2

Summary
This host is running Joomla! and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 3.8.11
Fixed version: 3.8.12
Installation path: /joomla/

Solution
Solution type: VendorFix
Upgrade to version 3.8.12 or later.

Affected Software/OS
Joomla! CMS versions 1.5.0 through 3.8.11

Vulnerability Insight
The following vulnerabilities exist:
- Inadequate output filtering on the user profile page could lead to a stored XSS attack. (CVE-2018-15880)
- Inadequate checks in the InputFilter class could allow specifically prepared PHAR files to pass the upload filter. (CVE-2018-15882)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Joomla! < 3.8.12 Multiple Vulnerabilities (ODD: 1.3.6.1-4.1.25623.1.0.112371)
Version used: \$Revision: 12252 \$

References
CVE: CVE-2018-15880, CVE-2018-15882
Other: <https://developer.joomla.org/security-centre/744-20180802-core-stored-xss-vulnerability-in-the-frontend-profile.html>
<https://developer.joomla.org/security-centre/743-20180801-core-hardening-the-inputfilter-for-phar-stubs.html>
<https://www.joomla.org>

Details of a vulnerability that was found during a scan.



Report: Results (65 of 1809)

Vulnerability	Severity	QoD	Host
OS End of Life Detection	10.0 (High)	80%	147.2
OS End of Life Detection	10.0 (High)	80%	147.2
OS End of Life Detection	10.0 (High)	80%	147.2
Joomla! < 3.8.12 Multiple Vulnerabilities	7.5 (High)	80%	147.2
Joomla! < 3.8.12 Multiple Vulnerabilities	7.5 (High)	80%	147.2
Joomla! < 3.8.12 Multiple Vulnerabilities	7.5 (High)	80%	147.2
Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities	7.5 (High)	80%	147.2
Report default community names of the SNMP Agent	7.5 (High)	99%	147.2
Joomla! < 3.8.13 Multiple Vulnerabilities	6.5 (Medium)	80%	147.2
Joomla! < 3.8.13 Multiple Vulnerabilities	6.5 (Medium)	80%	147.2
Joomla! < 3.8.13 ACL Violation Vulnerability	6.5 (Medium)	80%	147.2
Joomla! < 3.8.13 ACL Violation Vulnerability	6.5 (Medium)	80%	147.2
Joomla! < 3.8.13 RCE Vulnerability	6.5 (Medium)	80%	147.2
Joomla! < 3.8.13 RCE Vulnerability	6.5 (Medium)	80%	147.2

Prioritized list of vulnerabilities found during a scan.



Scan dashboard showing scan status and overview of vulnerabilities found.

ABOUT 3ROX

3ROX, a regional Research and Education (R&E) Network, operates and manages network infrastructure that connects many universities and schools in Pennsylvania and West Virginia to R&E networks and the commodity Internet. Our primary audience is education (both K-12 and higher), museums, libraries and other non-profits although we can provide services to “for-profit” organizations as well. A major benefit of working with 3ROX, which has been providing Internet services for over 25 years, is that we pool the networking requirements of many different groups and offer services that are less expensive and more stable than they could obtain on their own. 3ROX is part of a education institution and understands the unique needs and demands that those institutions often have.

FOR MORE INFORMATION ON 3ROX AND OTHER RESEARCHSOC SERVICES, CONTACT RESEARCHSOC
<https://researchsoc.iu.edu/contact/index.html>