


Vulnswatch lets you track the known and published vulnerabilities in third party components of your system. It works as a website for you.

















Once you register, you have to provide a short description of your system under monitoring. This description is called a project.

A screenshot of the 'Editing Project' form in the vulnswatch application. The form is titled 'Editing Project' and has a navigation bar at the top with links for 'Relevant Vulnerabilities', 'All Vulnerabilities', 'Projects', 'Reactions', and 'Zaur'. The form contains three input fields: 'Name' with the value 'North-west Server', 'Describe it in few words, please:' with the value 'The corporate server of the North-west branch', and 'Components:' with the value 'OpenBSD, nginx, Rails, openssl, vsftpd'. At the bottom of the form is a blue 'Update Project' button.

After the description is provided vulnswatch searches the database with CVEs and presents you with the findings.


 vulnswatch Relevant Vulnerabilities All Vulnerabilities Projects Reactions Zaur ▾

Search in names, components or summary Clear Search

















Name	Updated ▾	Component	Summary	Details	Project	Reaction
<input type="checkbox"/> CVE-2018-...		<input type="text" value="e.g. BSD"/>	<input type="text" value="e.g. Apache 2"/>		<input type="text" value="at least on"/>	<input type="text"/>
<input type="checkbox"/> CVE-2016-3693	6 days ago		The Safemode gem before 1.2.4 for Ruby, when initialized with a delegate object that ...	  	Rails in North-west Server	
<input type="checkbox"/> CVE-2014-3566	8 days ago		The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nond...	  	openssl in North-west Server	
<input type="checkbox"/> CVE-2018-1299	23 days ago		In Apache Allura before 1.8.0, unauthenticated attackers may retrieve arbitrary files...	  	nginx in North-west Server	
<input type="checkbox"/> CVE-2017-3735	25 days ago		While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to...	  	openssl in North-west Server	

Next the user can research the vulnerabilities reading their summary or clicking one of the three icons in the Details column: NVD page, Cve Details page or google search about the CVE will show up.

Managing the findings comes next. In the Reaction column the user can specify what happens with the findings. This column tells if the findings are false positives, present a problem, are in an unknown, not yet researched state, Or indicate that the problem has been solved already.

 vulnswatch Relevant Vulnerabilities All Vulnerabilities Projects Reactions Zaur ▾

Search in names, components or summary Clear Search

Name	Updated ▾	Component	Summary	Details	Project	Reaction
<input type="checkbox"/> CVE-2018-...		<input type="text" value="e.g. BSD"/>	<input type="text" value="e.g. Apache 2"/>		<input type="text" value="at least on"/>	<input type="text"/>
<input type="checkbox"/> CVE-2016-3693	6 days ago		The Safemode gem before 1.2.4 for Ruby, when initialized with a delegate object that ...	  	Rails in North-west Server	
<input type="checkbox"/> CVE-2014-3566	8 days ago		The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nond...	  	openssl in North-west Server	
<input type="checkbox"/> CVE-2018-1299	23 days ago		In Apache Allura before 1.8.0, unauthenticated attackers may retrieve arbitrary files...	  	nginx in North-west Server	
<input type="checkbox"/> CVE-2017-3735	25 days ago		While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to...	  	openssl in North-west Server	

Like this we achieve the management of known and big vulnerabilities in third-party components of a system.

What is it good for?

- It can be used with any system: a server, a software project, a whole network of an organization...
- It allows management and tracking of vulnerabilities
- It does not require any coding skills or installing anything, e.g. Dependency Check is more precise, but is targeted for developers
- It allows for exchange between people on findings.