Nimbusec Website Security Monitor Issue Types 2026

Malware

Name	Event	Description
Malware	malware	Malicious code fragments are found on a Web page. Typical examples would be, amongst others, credit card skimmers, crypto miners or tech scams.
SEO-Spam	seospam	If changes on a website are detected while acting as 'googlebot' instead of the default browser agent a warning for suspicious behavior is created

Web Shell

Web Shell	webshell	Malicious code patterns are found in source files based on behaviour patters and signature database of the Nimbusec server agent

Application

Outdated Application	cms-version	An application running on an outdated verrsion has been found on the website
Vulnerable Application	cms-vulnerable	An application with a possible vulnerability has been found on the website
CMS Tampered	cms-tampered	Core file of WordPress change and are only generated by Nimbusec's server agent. However, Nimbusec cannot not distinguish between legitimate and malicious changes.

TLS

TLS Protocol	tls-protocol	Unsafe TLS protocol allowed in configuration
TLS Ciphersuite	tls-ciphersuite	Unsafe TLS cipher allowed in configuration
TLS Sigalg	tls-sigalg	Outdated hash algorithm was used in the creation of the certificate
TLS Notrust	tls-notrust	Untrasted root certificate
TLS Hostname	tls-hostname	Hostname or alternative name does not match the certificate
TLS Expires	tls-expires	The TLS certificate will expire soon or has already expired
TLS Legacy	tls-legacy	Symantec legacy certificate in use
TLS Misconfigured Chain	tls-misconfigured-chain	The received certificate chain was incomplete or misconfigured
TLS Revoked Cert	tls-revoked-cert	The certificate was revoked
No HTTPS Redirect	no-https-redirect	HTTP website does not redirect to HTTPS

Content

Defacement	defacement	The visual appearance of a website was changed to distribute social, political or just for fun messages to the visitor
Content Violation	content-violation	Changes of the content of a Web page are detected. These change may be intended by the website owner or may be the result of a malicious attack. However, Nimbusec does not distinguish between legitimate and malicious changes.

Blacklist

Blacklist	blacklist	The domain which is subject to review is found on blacklists monitored by Nimbusec

Reputation

Suspicious Link	suspicious-link-v2	Suspicious resources, based on blacklists monitored by Nimbusec, are embedded (but not loaded) on a Web page. A typical example of this type of event would be a link (a-tag) which points to a suspicious domain found in the Nimbusec blacklist.
Suspicious Request	suspicious-request	A suspicious resource, based on blacklists monitored by Nimbusec, is actively loaded by a Web page. A typical example of this type of event would be a JavaScript source which points to a suspicions domain.

Configuration

opendir	config-opendir	When a web server's directory listing is enabled, anyone can browse the contents of folders (e.g., `/files/`) instead of being restricted to specific pages.
php Error	config-phperror	When PHP error messages are shown directly to users instead of being logged securely.
public config	config-public	Apache status pages are checked for public accesibillity.
Security Header config	config-secheads	Will be shown if SHR rating is grade "D" or lower. (missing or improperly configured HTTP security headers, such as Content-Security-Policy, Stricy-Transport-Security or X-Frame-Options)
Deprecated Header	config-header-deprecated	The server uses outdated headers that are no longer recommended. They should be replaced with modern alternatives for better security and compatibility.

Text

SRI Missing	sri-missing	No integrity hash is defined for the external resource.
SRI Invalid	sri-invalid	The provided hash does not match the actual content of the loaded file.

Hijack Link	hijack-link	The destination domain of the link is not (or no longer) registered. Attackers can register this address to redirect users to malicious or phishing content.
Hijack Resource	hijack-resource	The source domain of the resource is not registered. A third party can claim the domain to inject malicious scripts or assets directly into the website.

Revision #25
Created 22 October 2024 07:34:27 by Test Editor
Updated 1 June 2026 09:46:41 by Test Editor