Issue and Event overview

Nimbusec Website Security Monitor

Issue Types 2022

Category	Issue Types	Descritpion
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	If changes on a website are detected while acting as 'googlebot' instead of the default browser agent a warning for suspicious behavior is thrown
Defacement	Defacement	The visual appearance of a website was changed to distribute social, political or just for fun messages to the visitor
	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.
Reputation	Blacklist	The domain which is subject to review is found on blacklists monitored by Nimbusec
	Suspicious Link	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	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.
Webshell	Webshell	Malicious code fragments are found in files monitored by Nimbusec's Server Agent. As files are directly inspected on the Web server additional malicious code such as Webshells may be detected.
Application	Vulnerable	An application with a possible vulnerability has been found on a website
	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.
	Outdated	An outdated application has been found on a website
TLS	TLS Expires	The TLS certificate will expire soon
	TLS Notrust	Untrusted root certificate
	TLS Protocol	Unsafe TLS protocol allowed in configuration
	TLS Sigalg	Bad signature algorithm
	TLS Ciphersuite	Unsafe TLS cipher allowed in configuration
	TLS Hostname	Hostname does not match certificate
	TLS Legacy	Symantec legacy certificate in use
	TLS Misconfigured Chain	The received certificate chain was incomplete or misconfigured
	TLS No Https redirect	HTTP website does not redirect to HTTPS
	TLS Revoked Cert	The certificate was revoked by the owner
Configuration	Baseline Empty	Wrong Agent configuration: empty result

Revision #1
Created 16 September 2022 04:53:44 by Patrick Wall
Updated 16 September 2022 05:02:45 by Patrick Wall