PCI-DSS-SCAN_2

Report generated by Nessus™ Thu, 17 Nov 2022 20:44:29 EST

TABLE OF CONTENTS

Overview

Top 10 Critical Vulnerabilities

Top 10 High Vulnerabilities

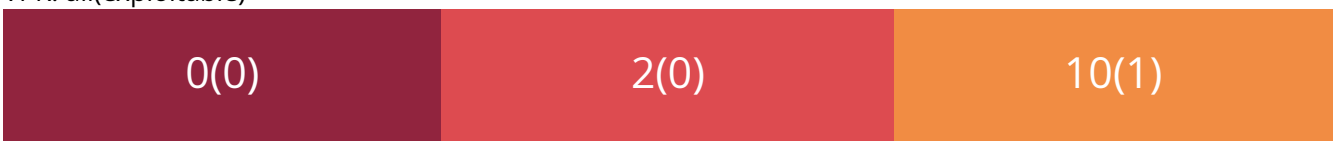
Top 10 Most Prevalent Vulnerabilities

Overview

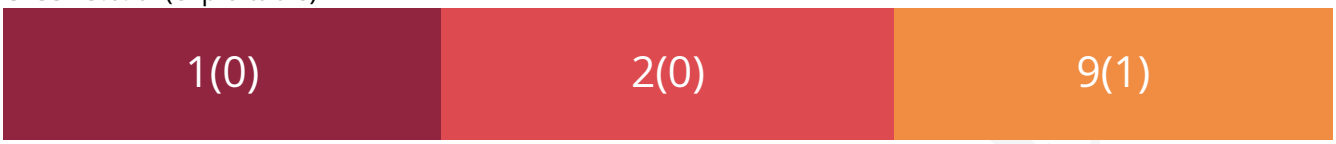
The Overview section contains two matrices that provide summary counts, by severity, using VPR or CVSS. Within each cell there is a number for the vulnerability count, and in parentheses the count of exploitable vulnerabilities. Also provided is the count based on severity level.

Vulnerability Instances: all and exploitable, by severity

VPR: all(exploitable)



CVSS v3.0: all(exploitable)



Top 10 Critical Vulnerabilities

The two tables in this chapter provide a top 10 vulnerabilities grouped using the critical VPR or critical CVSS. For VPR and CVSS v3.0 the rating is 9.0 - 10, for CVSS v2.0 the rating is 10. The vulnerabilities identified using VPR are the most active in the wild, and based on an in-depth threat analysis, are considered the most critical to mitigate. Traditionally, the method for identifying risk was most commonly with CVSS v3.0 or CVSS v2.0. While each still remain very important, and should be mitigated, these vulnerabilities are not given the same context as VPR identified vulnerabilities.

No Results:

No Top 10 Critical Vulnerabilities: (VPR) Found

Top 10 Critical Vulnerabilities: (CVSS v3.0)

Top 10 most prevalent critical vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	9.8	-	2022/03/02	1

* indicates the v3.0 score was not available; the v2.0 score is shown

Top 10 High Vulnerabilities

The two tables in this chapter provide a top ' + limit + ' vulnerabilities grouped using the High VPR or High CVSS. For VPR and CVSS v3.0 the rating is 7.0 - 8.9, for CVSS v2.0 the rating is 7.0 - 9.9. The vulnerabilities identified using VPR are the most active in the wild and based on an in-depth threat analysis are considered the most critical to mitigate. Traditionally, the method for identifying risk was most commonly with CVSS v3.0 or CVSS v2.0. While each still remain very important, and should be mitigated, these vulnerabilities are not given the same context as VPR identified vulnerabilities.

Top 10 High Vulnerabilities: (VPR)

Top 10 most prevalent high vulnerabilities

Plugin ID	Plugin Name	Plugin Family	VPR	Known Exploit?	Publication Date	Count
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	8.4	-	2022/03/02	1

Top 10 High Vulnerabilities: (CVSS v3.0)

Top 10 most prevalent high vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
17693	Apache mod_suexec Multiple Privilege Escalation Vulnerabilities	Web Servers	7.0	-	2007/04/11	1
33929	PCI DSS compliance	Policy Compliance	*	-	2008/08/07	1

* indicates the v3.0 score was not available; the v2.0 score is shown

Top 10 Most Prevalent Vulnerabilities

The two tables in this chapter provide a top 10 vulnerabilities grouped using the Medium through Critical. For VPR, CVSS v3.0, and CVSS v2.0 the rating is 4.0 - 10. The vulnerabilities identified using VPR are the most active in the wild and based on an in-depth threat analysis are considered the most critical to mitigate. Traditionally, the method for identifying risk was most commonly with CVSS v3.0 or CVSS v2.0. While each still remain very important, and should be mitigated, these vulnerabilities are not given the same context as VPR identified vulnerabilities.

Top 10 Most Prevalent Vulnerabilities: (VPR)

Top 10 most prevalent (medium, high, critical) vulnerabilities

Plugin ID	Plugin Name	Plugin Family	VPR	Known Exploit?	Publication Date	Count
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	8.4	-	2022/03/02	1
17693	Apache mod_suexec Multiple Privilege Escalation Vulnerabilities	Web Servers	5.9	-	2007/04/11	1
17695	Apache Mixed Platform AddType Directive Information Disclosure	Web Servers	4.2	Yes	2007/12/19	1

Top 10 Most Prevalent Vulnerabilities: (CVSS v3.0)

Top 10 most prevalent (medium, high, critical) vulnerabilities

Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	9.8	-	2022/03/02	1
17693	Apache mod_suexec Multiple Privilege Escalation Vulnerabilities	Web Servers	7.0	-	2007/04/11	1
33929	PCI DSS compliance	Policy Compliance	*	-	2008/08/07	1
17695	Apache Mixed Platform AddType Directive Information Disclosure	Web Servers	5.6	Yes	2007/12/19	1
40984	Browsable Web Directories	CGI abuses	5.3	-	2009/09/15	1
56208	PCI DSS Compliance : Insecure Communication Has Been Detected	Policy Compliance	5.3	-	2011/09/15	1
88099	Web Server HTTP Header Information Disclosure	Web Servers	5.3	-	2016/01/22	1
88490	Web Server Error Page Information Disclosure	Web Servers	5.3	-	2016/01/29	1
106232	Apache ServerTokens Information Disclosure	Web Servers	5.3	-	2018/01/22	1
121041	Sensitive File Disclosure	CGI abuses	5.3	-	2019/01/09	1

* indicates the v3.0 score was not available; the v2.0 score is shown