tenable Nessus

owaspbwa

Report generated by Tenable Nessus™

Sat, 09 Aug 2025 18:08:44 EDT

TABLE OF CONTENTS

Hosts with Vulnerabilities > 1 Year Old Report

Hosts with Vulnerabilities > 1 Year Old Report

Any vulnerabilities create gaps in the network's integrity, which attackers can take advantage of to gain access to the network. Once inside the network, an attacker can perform malicious attacks, steal sensitive data, and cause significant damage to critical systems. The longer a vulnerability exists, the more likely it can be easily compromised. This report provides a summary of the most prevalent vulnerabilities published more than a year ago. Note, the data shown in these tables is based on "vulnerability publication date", not to be confused with the "plugin publication date". Both of these dates can be seen when the plugin details link is accessed.

Hosts with Vulnerabilities > 1 Year Old: Top 25

Hosts with Vulnerabilities > 1 Year Old: Top 25 table organizes the most prevalent vulnerabilities detected. The data is sorted using the count, which is a representation of the affected hosts. While some plugins may be present more than one time on a single host, for the most part a plugin will only be present once on each host. This list of vulnerabilities exposes the organization to many different attack frameworks and script kiddie attacks. The longer a vulnerability has existed, the more people become aware of it, and can result in more script kiddie attacks. These vulnerabilities should be prioritized and the software removed or updated to a supported version as soon as possible.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Count
CRITICAL	15780	phpBB viewtopic.php highlight Parameter SQL Injection (ESMARKCONANT)	2
CRITICAL	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)	2
HIGH	11938	phpBB < 2.0.7 Multiple Script SQL Injection	2
HIGH	13655	phpBB < 2.0.9 Multiple Vulnerabilities	2
MEDIUM	11213	HTTP TRACE / TRACK Methods Allowed	2
MEDIUM	13840	phpBB < 2.0.10 Multiple XSS	2
MEDIUM	17205	phpBB <= 2.0.11 Multiple Vulnerabilities	2
MEDIUM	17301	phpBB <= 2.0.13 Multiple Vulnerabilities	2
MEDIUM	18124	phpBB <= 2.0.14 Multiple Vulnerabilities	2
MEDIUM	29745	WordPress 'query.php' is_admin() Function Information Disclosure	2
MEDIUM	46803	PHP expose_php Information Disclosure	2
MEDIUM	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	2
MEDIUM	88098	Apache Server ETag Header Information Disclosure	2
MEDIUM	136929	JQuery 1.2 < 3.5.0 Multiple XSS	2
LOW	18626	phpBB < 2.0.17 Nested BBCode URL Tags XSS	2
HIGH	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	1
HIGH	90509	Samba Badlock Vulnerability	1
MEDIUM	35291	SSL Certificate Signed Using Weak Hashing Algorithm	1

MEDIUM	42982	AWStats < 6.95 awredir.pl Arbitrary Site Redirect	1
MEDIUM	57608	SMB Signing not required	1
MEDIUM	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	1
LOW	10114	ICMP Timestamp Request Remote Date Disclosure	1
LOW	70658	SSH Server CBC Mode Ciphers Enabled	1
LOW	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	1

Hosts with Vulnerabilities > 1 Year Old: Hosts by Plugin

Hosts with Vulnerabilities > 1 Year Old: Hosts by Plugin table provides the IT operations team with an action plan and the identified hosts for each vulnerability. IT managers are able to use this information in planning patch deployments and in working with the information security team in risk mitigation efforts. The table provides all detected vulnerabilities and sorts the scan results using severity, then plugin ID. The entries in the "Hosts" column are then sorted in ascending order.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Hosts
CRITICAL	15780	phpBB viewtopic.php highlight Parameter SQL Injection (ESMARKCONANT)	172.20.10.4
CRITICAL	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)	172.20.10.4
HIGH	11938	phpBB < 2.0.7 Multiple Script SQL Injection	172.20.10.4
HIGH	13655	phpBB < 2.0.9 Multiple Vulnerabilities	172.20.10.4
MEDIUM	11213	HTTP TRACE / TRACK Methods Allowed	172.20.10.4
MEDIUM	13840	phpBB < 2.0.10 Multiple XSS	172.20.10.4
MEDIUM	17205	phpBB <= 2.0.11 Multiple Vulnerabilities	172.20.10.4
MEDIUM	17301	phpBB <= 2.0.13 Multiple Vulnerabilities	172.20.10.4
MEDIUM	18124	phpBB <= 2.0.14 Multiple Vulnerabilities	172.20.10.4
MEDIUM	29745	WordPress 'query.php' is_admin() Function Information Disclosure	172.20.10.4
MEDIUM	46803	PHP expose_php Information Disclosure	172.20.10.4
MEDIUM	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	172.20.10.4

MEDIUM	88098	Apache Server ETag Header Information Disclosure	172.20.10.4
MEDIUM	136929	JQuery 1.2 < 3.5.0 Multiple XSS	172.20.10.4
LOW	18626	phpBB < 2.0.17 Nested BBCode URL Tags XSS	172.20.10.4
HIGH	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	172.20.10.4
HIGH	90509	Samba Badlock Vulnerability	172.20.10.4
MEDIUM	35291	SSL Certificate Signed Using Weak Hashing Algorithm	172.20.10.4
MEDIUM	42982	AWStats < 6.95 awredir.pl Arbitrary Site Redirect	172.20.10.4
MEDIUM	57608	SMB Signing not required	172.20.10.4
MEDIUM	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	172.20.10.4
LOW	10114	ICMP Timestamp Request Remote Date Disclosure	172.20.10.4
LOW	70658	SSH Server CBC Mode Ciphers Enabled	172.20.10.4
LOW	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	172.20.10.4