Weekly Zero-Day Vulnerability Coverage Bulletin

(18th February – 24th February)

Summary:

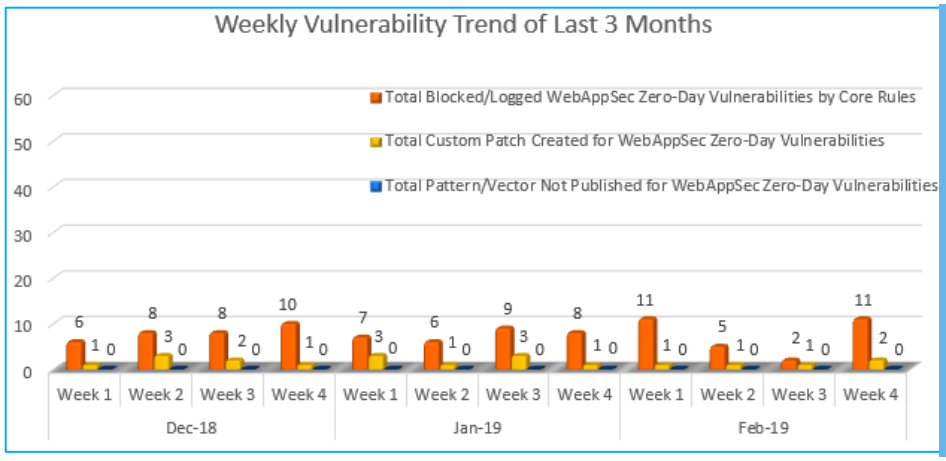
Total **13 Zero-Day Vulnerabilities** were discovered in **7 Categories** this week

3	2	1	4	1	1	1
Cross Site Scripting	SQL Injection	Command Injection	Directory Traversal	File Injection	Malicious File Upload	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	11
Zero-Day Vulnerabilities Protected through Custom Rules	2*
Zero-Day Vulnerabilities for which protection cannot be determined	0**

* To enable custom rules please contact support@indusface.com
** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

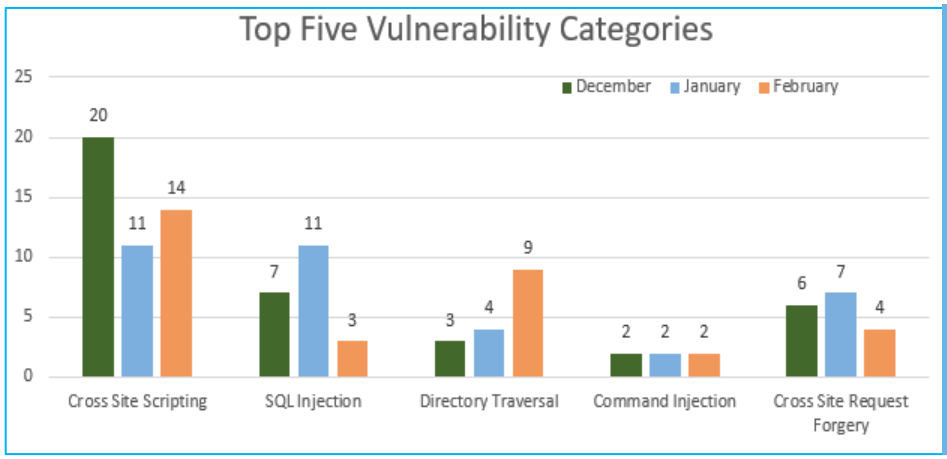
Vulnerability Trend:



Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

82% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

18% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting vulnerabilities were discovered in December compared to other months and categories so far.

Medium no. of SQL Injection and CSRF attacks was found in all the months.

Note: Our Sig-Dev team constantly monitors the security landscape and leading security websites to identify any new vulnerabilities identified/published and monitors/updates rules to ensure around the clock protection for customer sites.

Details:

S. No.	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage
1.	Cross Site Scripting	CVE-2019-8435	PHPMyWind 5.5 admin/default.php HTTP Host Header cross site scripting	A vulnerability was found in PHPMyWind 5.5. It has been rated as problematic. This issue affects some processing of the file *admin/default.php*. The manipulation as part of a *HTTP Host Header* leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance and would make it possible to initiate further attacks.	Protected by Default Rules.
		CVE-2019-8425	ZoneMinder up to 1.32.2 SQL-ERR Message includes/database.php cross site scripting	A vulnerability classified as problematic has been found in ZoneMinder up to 1.32.2 (Video Surveillance Software). This affects an unknown function of the file *includes/database.php* of the component *SQL-ERR Message Handler*. The manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
		CVE-2019-8953	HAProxy Package up to 0.59 on pfSense haproxy_listeners.php desc/table_actionsaclN cross site scripting	A vulnerability, which was classified as problematic, was found in HAProxy Package up to 0.59 on pfSense (Firewall Software). This affects a function of the file *haproxy_listeners.php*. The manipulation of the argument desc/table_actionsaclN with the input value "><script>alert("test")</script> leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject	Protected by Default Rules.

				arbitrary html and script code into the website.	
2.	SQL Injection	CVE-2019-8429	ZoneMinder up to 1.32.2 ajax/status.php filter[Query][terms][0][cnj] sql injection	A vulnerability has been found in ZoneMinder up to 1.32.2 (Video Surveillance Software) and classified as critical. Affected by this vulnerability is a functionality of the file *ajax/status.php*. The manipulation of the argument filter[Query][terms][0][cnj] as part of a *Parameter* leads to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements.	Protected by Default Rules.
		CVE-2019-8428	ZoneMinder up to 1.32.2 control.php groupSql sql injection	A vulnerability, which was classified as critical, was found in ZoneMinder up to 1.32.2 (Video Surveillance Software). Affected is a function of the file *skins/classic/views/control.php*. The manipulation of the argument groupSql as part of a *Parameter* leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	Protected by Default Rules.
3.	Directory Traversal	CVE-2019-8412	FeiFeiCms 4.0.181010 on Windows index.php directory traversal	A vulnerability classified as critical was found in FeiFeiCms 4.0.181010 on Windows (Content Management System). Affected by this vulnerability is the functionality of the file *index.php?s=Admin-Data-Down-id-..*. The manipulation with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As	Protected by Default Rules.

			an impact it is known to affect confidentiality, integrity, and availability. The weakness was released 02/17/2019. This vulnerability is known as CVE-2019-8412 since 02/17/2019. The attack can be launched remotely.	
	NA	Magento Patches Command Execution, Local File Read Flaws	Both of vulnerabilities need low privileges admin account, usually given to Marketing users : The first vulnerability is a command execution using path traversal, and requires the user to be able to create products The second vulnerability is a local file read, and requires the user to be able to create email templates.	Protected by Default Rules.
	CVE-2019-6340	Critical flaw in Drupal allows Remote Code Execution	Some field types do not properly sanitize data from non-form sources. This can lead to arbitrary PHP code execution in some cases. A site is only affected by this, if one of the following conditions are met: The site has the Drupal 8 core RESTful Web Services (rest) module enabled and allows GET, PATCH or POST requests, or the site has another web services module enabled, like JSON:API in Drupal 8, or Services or RESTful Web Services in Drupal 7.	Protected by Default Rules.
	NA	Security experts disclosed a critical remote code execution vulnerability in versions of WordPress	An attacker who gains access to an account with at least author privileges on a target WordPress site can execute arbitrary PHP code on the underlying server, leading to a full remote takeover. We sent the WordPress security team details about another vulnerability in the WordPress core that can give attackers exactly	Protected by Default Rules.

				such access to any WordPress site, which is currently unfixed.	
		CVE-2019-8412	FeiFeiCms 4.0.181010 on Windows index.php directory traversal	A vulnerability classified as critical was found in FeiFeiCms 4.0.181010 on Windows (Content Management System). Affected by this vulnerability is the functionality of the file *index.php?s=Admin-Data-Down-id-..*. The manipulation with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was released 02/17/2019. This vulnerability is known as CVE-2019-8412 since 02/17/2019. The attack can be launched remotely.	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2019-8902	idreamsoft iCMS up to 7.0.14 public/api.php cross site request forgery	A vulnerability classified as problematic was found in idreamsoft iCMS up to 7.0.14 (Content Management System). Affected by this vulnerability is the functionality of the file *public/api.php?app=user*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. As an impact it is known to affect integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was disclosed in 02/18/2019.	Protected by Custom Rules.

5.	Command Injection	NA	Expert released a PoC for a remote code execution flaw in mIRC App	mIRC is a popular Internet Relay Chat application that allows users to chat by connecting to IRC servers, it also allows users to exchange files and links. Installing the mIRC application will create three custom URI schemes, irc:, ircs:, and mircurl: that can be used as links to launch mIRC (i.e. url irc://irc.undernet.org/). The flaw could be exploited by attackers to execute various commands, including download and install binaries on the vulnerable system. The flaw allows attackers to inject commands into these custom URI schemes, it affects mIRC versions older than 7.55.	Protected by Default Rules.
6.	File Injection	CVE-2019-8394	Zoho ManageEngine ServiceDesk Plus up to 10.0 Login Page File Upload privilege escalation	A vulnerability was found in Zoho ManageEngine ServiceDesk Plus up to 10.0. It has been classified as critical. Affected is code of the component *Login Page*. The manipulation with an unknown input leads to a privilege escalation vulnerability (File Upload). CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was presented 02/17/2019. The advisory is available at manageengine.com. This vulnerability is traded as CVE-2019-8394 since 02/16/2019.	Protected by Default Rules.
7.	Malicious File Upload	NA	Vulnerabilities Patched in WP Cost Estimation Plugin	WP Cost Estimation normally prevents users from uploading dangerous file types to the server, but a flaw in the plugin allowed them to upload	Protected by Custom Rules.

	malicious PHP files with an apparently harmless extension. The second flaw allows attackers to delete arbitrary files. In the attacks spotted by Wordfence, they deleted the wp-config.php file, which makes WordPress believe that a fresh install is taking place – since no database configuration is present – enabling the hacker to connect the site to their own database and log in as administrator.