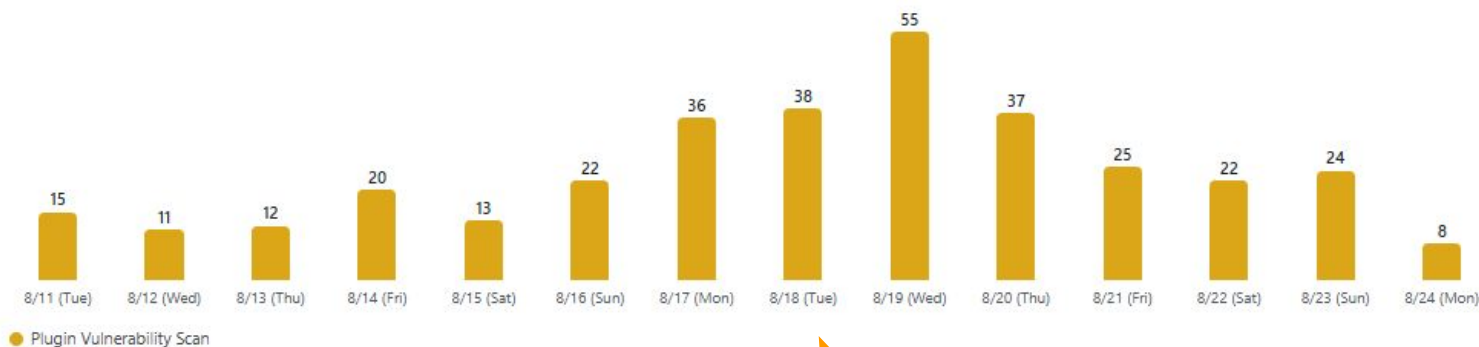


# Security Trend

## Security trend (Last 14 days) — Plugin Vulnerability Scan

Period Last 14 days Aggregation interval 1 day



## Attack summary for Last 14 days

The following counts show malicious attacks protected by this plugin.

All

High Volume Requests  
0 items

REST API Abuse  
22 items

Admin Area Hacking  
145 items

Plugin Vulnerability Scan  
341 items

Theme Vulnerability Scan  
39 items

WordPress Core Vulnerability Scan  
71 items

Config File Scan  
162 items

Backdoor Scan  
25 items

User Enumeration  
0 items

Malicious Query  
0 items

Suspicious 404 Flood  
82 items

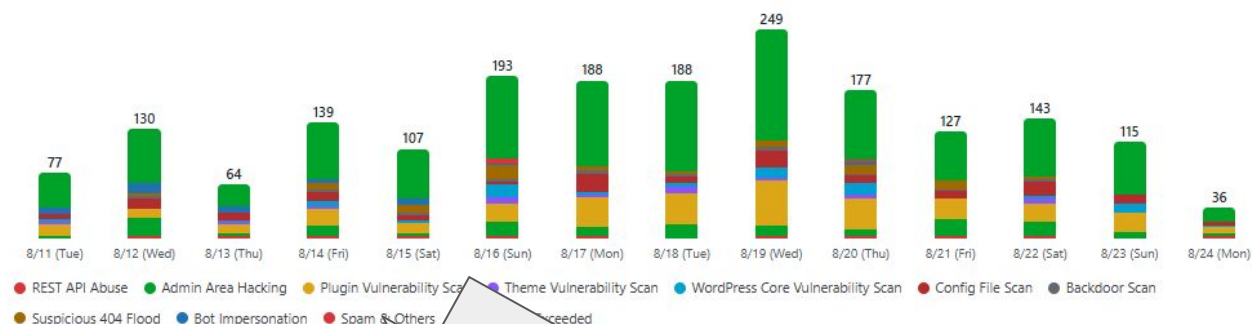
Scanner Tool  
0 items

Bot Impersonation  
71 items

Spam & Others  
8 items

Risk Score Exceeded  
1,039 items

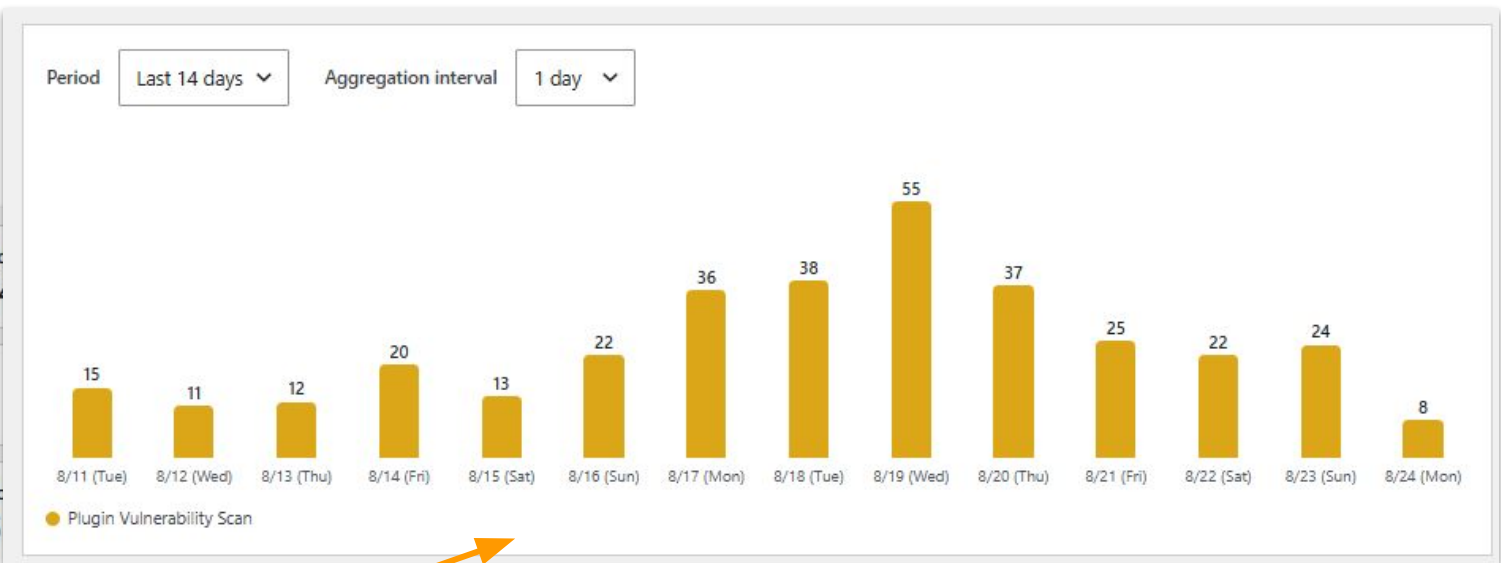
Period Last 14 days Aggregation interval 1 day



When you click "Plugin Vulnerability Scan," the graph also switches to display data for the "Plugin Vulnerability Scan."

「プラグイン脆弱性スキャン」をクリックするとグラフも「プラグイン脆弱性スキャン」のデータになる。

|                                               |                               |
|-----------------------------------------------|-------------------------------|
| High Volume Requests<br>0 items               | REST API Abuse<br>22 items    |
| WordPress Core Vulnerability Scan<br>71 items | Config File Scan<br>154 items |
| Suspicious 404 Flood<br>82 items              | Scanner Tool<br>0 items       |



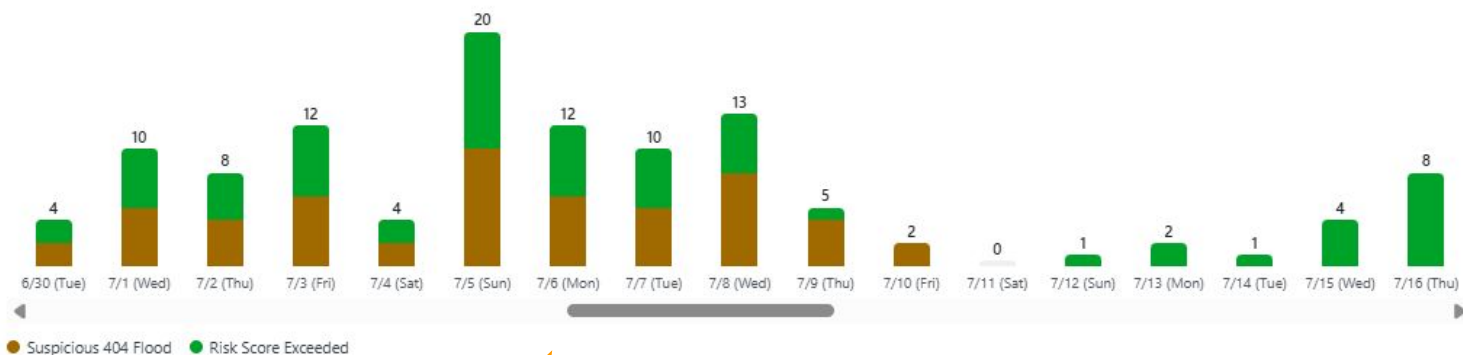
| Category                          | Detections |
|-----------------------------------|------------|
| High Volume Requests              | 0          |
| REST API Abuse                    | 22         |
| Admin Area Hacking                | 145        |
| <b>Plugin Vulnerability Scan</b>  | 341        |
| Theme Vulnerability Scan          | 39         |
| WordPress Core Vulnerability Scan | 71         |
| Config File Scan                  | 154        |
| Backdoor Scan                     | 25         |
| User Enumeration                  | 0          |
| Malicious Query                   | 0          |
| Suspicious 404 Flood              | 82         |
| Scanner Tool                      | 0          |
| Bot Impersonation                 | 58         |
| Spam & Others                     | 8          |
| Risk Score Exceeded               | 1,027      |

Clicking "Plugin Vulnerability Scan" under "Category" in the Attack Summary displays the graph for the plugin vulnerability scan.

Attack summary内の「Category」で「プラグイン脆弱性スキャン」をクリックしてもプラグイン脆弱性スキャンのグラフが表示される。

選択中のページ: [https://syn-c.jp/this\\_is\\_a\\_new\\_hello\\_world.php](https://syn-c.jp/this_is_a_new_hello_world.php)

[すべてのページに戻る](#)



#### ページ別アクセス（直近 90 日）

ページのURLをクリックすると、上の棒グラフとサマリーがそのページの直近分に切り替わります。

| ページ                                                                                                                                               | 件数    | カテゴリ                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------|-------|---------------------------------------------------------------------------------------------------------------------------------|
| <a href="https://syn-c.jp/wp-json/oembed/1.0/embed">https://syn-c.jp/wp-json/oembed/1.0/embed</a>                                                 | 8,029 | REST API Abuse (4,704), Risk Score Exceeded (1,679), High Volume Requests (1,646)                                               |
| <a href="https://syn-c.jp/wp-login.php">https://syn-c.jp/wp-login.php</a>                                                                         | 4,687 | Admin Area Hacking (1,574), Suspicious 404 Flood (1,129), Risk Score Exceeded (1,012), High Volume Requests (972)               |
| <a href="https://syn-c.jp/wp-admin/">https://syn-c.jp/wp-admin/</a>                                                                               | 4,277 | Admin Area Hacking (1,300), Risk Score Exceeded (1,051), Suspicious 404 Flood (992), High Volume Requests (934)                 |
| <a href="https://syn-c.jp/wp-admin/index.php">https://syn-c.jp/wp-admin/index.php</a>                                                             | 4,115 | Admin Area Hacking (1,218), Risk Score Exceeded (1,016), Suspicious 404 Flood (966), High Volume Requests (915)                 |
| <a href="https://syn-c.jp/wp-content/plugins/hellopress/wp_filemanager.php">https://syn-c.jp/wp-content/plugins/hellopress/wp_filemanager.php</a> | 781   | Plugin Vulnerability Scan (535), Risk Score Exceeded (132), Suspicious 404 Flood (112), High Volume Requests (2)                |
| <a href="https://syn-c.jp/js/line-numbers.js">https://syn-c.jp/js/line-numbers.js</a>                                                             | 769   | Suspicious 404 Flood (634), Risk Score Exceeded (133), High Volume Requests (2)                                                 |
| <a href="https://syn-c.jp/.env">https://syn-c.jp/.env</a>                                                                                         | 759   | Config File Scan (327), Risk Score Exceeded (202), Suspicious 404 Flood (173), High Volume Requests (53), Bot Impersonation (4) |
| <a href="https://syn-c.jp/admin.php">https://syn-c.jp/admin.php</a>                                                                               | 666   | Risk Score Exceeded (383), Suspicious 404 Flood (267), High Volume Requests (16)                                                |
| <a href="https://syn-c.jp/this_is_a_new_hello_world.php">https://syn-c.jp/this_is_a_new_hello_world.php</a>                                       | 566   | Risk Score Exceeded (461), Suspicious 404 Flood (105)                                                                           |
| <a href="https://syn-c.jp/wp-admin/js/">https://syn-c.jp/wp-admin/js/</a>                                                                         | 562   | Admin Area Hacking (183), Suspicious 404 Flood (157), Risk Score Exceeded (155), High Volume Requests (67)                      |
| <a href="https://syn-c.jp/wp-includes/assets/">https://syn-c.jp/wp-includes/assets/</a>                                                           | 491   | Suspicious 404 Flood (193), Risk Score Exceeded (193), WordPress Core Vulnerability Scan (83), High Volume Requests (22)        |
| <a href="https://syn-c.jp/wp-content/admin.php">https://syn-c.jp/wp-content/admin.php</a>                                                         | 475   | Suspicious 404 Flood (231), Risk Score Exceeded (221), High Volume Requests (23)                                                |
| <a href="https://syn-c.jp/classwithtostring.php">https://syn-c.jp/classwithtostring.php</a>                                                       | 472   | Risk Score Exceeded (256), Suspicious 404 Flood (204), High Volume Requests (12)                                                |

When you select a page under “Access by Page,” the log for that page is displayed in a graph. ページ別アクセスでページを選択すると、当該ページのログがグラフに表示される。