1. {% if vulns\_by\_plugin %}

# Vulnerabilities by Plugin

{% for p in vulns\_by\_plugin %}

## {{ p.plugin\_name }}

|  |  |  |
| --- | --- | --- |
| **Severity** | {% if p.severity == '4' %}  **Critical**  {% elif p.severity == '3' %}  **High**  {% elif p.severity == '2' %}  **Medium**  {% elif p.severity == '1' %}  **Low**  {% elif p.severity == '0' %}  **Info**  {% endif %} | |
| **Plugin Family** | {{ p.plugin\_family }} | |
| **CVE** | {{ p.cve }} | |
| **Exploit** | Exp. Ease | {{ p.exploitability\_ease }} |
| Available | {{ p.exploit\_available }} |
| Metasploit | {{ p.metasploit\_name }} |
| CANVAS | {{ p.canvas\_name }} |
| **Description** | {{ p.description }} | |
| **Synopsis** | {{ p.synopsis }} | |
| **Solution** | {{ p.solution }} | |
| **Affected Systems:** |  | |
| **{%tr for a in p.addresses %}** | | |
| {{ a.address }} | {{ a.port }}/{{ a.protocol }} ( {{ a.service }} ) | |
| **{%tr endfor %}** | | |

{% endfor %}

{% endif %}