


Closed

 Opened 4 weeks ago by [muffinx](#)

X-Forwarded-For IP Spoofing/Faking

Dear E-Voting PIT Team

Now this one is not a "vulnerability", I think I found a way to spoof/fake IP's for logs. This could be used to spoof/fake one's IP when trying certain things out.

These were my first thoughts, but now during the writing of this report, I think this issue could also be used to attack certain functions.

Of course, the IP could be later investigated into the network logs, but still I want to report this one.

X-Forwarded-For is all over the place in the REST API Backends:

```
@NotNull @Header(PARAMETER_X_FORWARDED_FOR) String xForwardedFor,
-----
@NotNull @Header(PARAMETER_X_FORWARDED_FOR) String xForwardedFor,
```

It will be passed to these two functions:

./evoting-solution-master/source-code/online-voting-channel/ov-api-gateway/ag-ws-rest/src/main/java/com/scytl/products/ov/ag/ui/ws/rs/proxy/XForwardedForFactoryImpl.java

```
@Override
public String newXForwardedFor(final HttpServletRequest request) {
    String remoteAddresses = request.getHeader(HEADER);
    if (remoteAddresses == null) {
        remoteAddresses = request.getRemoteAddr();
    }
    String localAddress = request.getLocalAddr();
    return remoteAddresses + ',' + localAddress;
}
```

evoting-solution-master/source-code/online-voting-channel/ov-commons/ov-commons-lib/src/main/java/com/scytl/products/ov/commons/util/HttpRequestService.java:

```
public String getIpClientAddress(final HttpServletRequest request) {
    String address = request.getRemoteAddr();
    String xForwardedFor = request.getHeader(HTTP_HEADER_X_FORWARDED_FOR);
    if (xForwardedFor != null && !xForwardedFor.isEmpty()) {
        int index = xForwardedFor.indexOf(',');
        if (index > 0) {
            address = xForwardedFor.substring(0, index);
        } else {
            address = xForwardedFor;
        }
    }
    return address;
}
```

Now in both HttpServletRequest is directly used, and it looks after "X-Forwarded-For", which can be modified by the client. getIpClientAddress() will always be used like this:

```
// transaction id generation
transactionInfoProvider.generate(tenantId, httpRequestService.getIpClientAddress(
    httpRequestService.getIpServer(request));
```

and newXForwardedFor() like this:

```
String xForwardedFor = xForwardedForFactory.newXForwardedFor(request);
```

newXForwarded will be used for all kinds of operations.

Now to be honest with you there are so many places where this code is being used, that we can't really say just yet what the impact is.

I hope you understand this, since the source is really huge, there is a lot of code reusage and its pretty much hard to tell what all the functionalities are doing without a working instance.

But please take this one, once again serious.


Thank you very much for reading my report.

Best Regards

Anthony Schneider aka. muffinx Jannis Kirschner aka. xorkiwi



Swisspost @swisspost added In Progress topic: general labels 4 weeks ago




Swisspost @swisspost · 4 weeks ago

Maintainer

Hello Anthony,

Thank you very much for your input. We will verify this and get back to you.

Kind regards



muffinx @muffinx · 2 weeks ago

Guest

Dear E-Voting PIT Team

Do you have any update on this issue? Now we can perfectly understand that is one is a hard one, since we explained it pretty in a broad area. But we would like to get an update on this problem.


Unfortunately we can't yet really say where this affects the application, the source code is just too big, even after 2 weeks of researching, we are still in the beginning.

Even though, we think that this bug could have serious implications on all operations which do something with the client IP. That could result all kinds of manipulation(s), so a more secure way to get the client IP would be to use a java internal which takes the IP from the IP Header, instead of taking it from a manipulable HTTP header.

Thanks for you answers!

Best Regards

Anthony Schneider aka. muffinx Jannis Kirschner aka. xorkiwi



Swisspost @swisspost · 2 weeks ago

Maintainer


Hello you two,

Sorry for the late response.


Your observation sounds very interesting. We propose that you try this attack in the public intrusion test (which starts today). If you manage to spoof IP addresses that will appear in the Logs, this will probably count at least as a best practice finding.

Thank you

Kind regards



Swisspost @swisspost added topic: infrastructure label and removed In Progress topic: general labels 1 week ago



Swisspost @swisspost · 1 week ago

Maintainer

Hello you two,

Thank you for your submission over the platform for the public intrusion test. We will continue tracking this finding on the other platform, which means we are closing your issue here.

You will hear from us concerning the issue opened on the PIT platform.

Thank you for your understanding.

Kind regards



Swisspost @swisspost closed 1 week ago



muffinx @muffinx · 1 week ago

Guest

Dear E-Voting PIT Team

We first reported the X-Forwarded-For Issue around 3 weeks ago. We clearly described the problem and when reading the code it was obvious that this works.

After 2 weeks of no answer on the issue on gitlab, at the beginning of the PIT, we got a small answer "yes just try it out on the PIT".

So we created on the same day a proof-of-concept, now a whole week has passed and we have no idea what is going on.

To be honest, this is not what we call good cooperation, we actually work for you, so we ask you to give us minimal respect.

We understand that bureaucracy and administration takes it's time, but we think it should be doable in 1-3 weeks. And we aren't slowing down on purpose as a political move, right?

So we would like to see progress and a publication this week.

Thank you very much, we nevertheless hope for a good cooperation.

Best Regards

Anthony Schneiter aka. muffinx Jannis Kirschner aka. xorkiwi



Swisspost @swisspost · 1 week ago

Maintainer

Hello you two,

I am sorry for the waiting time. I understand completely your view of things, I will verify this for you and give you a proper feedback later today.

Kind regards



Swisspost @swisspost · 1 week ago

Maintainer

Hello you two,

I talked internally and the whole communication will be over the PIT platform.

In any case you do not hear in the next days please do not hesitate to contact them or us.

Kind regards



Swisspost @swisspost added category: question label 4 days ago

PIT Submission #153

X-Forwarded-For IP Spoofing/Faking

Added by **muffinx** 14 days ago. Updated 6 days ago.

Status: **ACCEPTED**
Priority: Normal
Assignee: level_1
Category: BEST PRACTICES

Description

Dear E-Voting PIT Team

So as we have described in:

<https://gitlab.com/swisspost/evoting-solution/issues/21>

The internal function to get the client ip can be manipulated by sending a malicious crafted X-Forwarded-For Header, Example:

X-Forwarded-For: 13.37.33.01, 13.37.33.01

We added this header during 2 x voting cycles at ov-api-gateway.

Please check in your logs if you can find somewhere the IP: 13.37.33.01

This was the IP we used for our proof-of-concept.

Thank you very much.

Best Regards

Anthony Schneiter aka. muffinx

Jannis Kirschner aka. xorkwi

x_forwarded_for (14.9 KB) SPOOFING REQUESTS muffinx, 25/02/2019 16:16

History

All Notes Changes

Updated by **level_1** 14 days ago

#2

Status changed from **NEW** to **TRIAGE**

Updated by **level_1** 14 days ago

#3

Status changed from **TRIAGE** to **INCOMPLETE**

Hello,

Thanks for submission. We are currently investigating this issue.

Could you provide more information about the request ?

We need the following details :

- IP
- Timestamp
- Method
- URI

If you do not have this data, you can provide them from a new spoofing attempt.

Regards.

--

SCRT Team

Updated by **muffinx** 14 days ago

#4

File x_forwarded_for added

Status changed from **INCOMPLETE** to **UPDATED**

Dear SCRT Team

I will provide you with the information you asked for.

IP: 13.37.33.01

The other information you can see in my requests, the timestamp you can take by the time of the response minus a few second.

Btw. wouldn't it be easier to grep for the IP I gave you in the first place?

In the attachments you can find the requests I done during the whole voting cycle.

In the whole cycle I tried to fake/spoof the IP with X-Forwarded-For.

Thanks for your answers.

Best Regards

Anthony Schneiter aka. muffinx

Jannis Kirschner aka. xorikiwi

Updated by **level_1** 14 days ago

#5

Status changed from **UPDATED** to **TRIAGE**

Updated by **level_1** 14 days ago

#7

Status changed from **TRIAGE** to **INVESTIGATING**

Assignee changed from **level_1** to **level_2**

Thanks you, we will keep you in touch about the investigation.

Best Regards.

--

SCRT Team

Updated by **muffinx** 14 days ago

#8

And btw. just to make sure your looking at the right place, I don't mean the tomcat logs.

I mean the logger in Scyl SecureLogger.

Thank you very much.

Best Regards

Anthony Schneider aka. muffinx

Jannis Kirschner aka. xorkiwi

Updated by **level_2** 12 days ago

#9

Assignee changed from **level_2** to **level_1**

Updated by **muffinx** 8 days ago

#11

Dear E-Voting PIT Team

We first reported the X-Forwarded-For Issue around 3 weeks ago.

We clearly described the problem and when reading the code it was obvious that this works.

After 2 weeks of no answer on the issue on gitlab, at the beginning of the PIT, we got a small answer "yes just try it out on the PIT".

So we created on the same day a proof-of-concept, now a whole week has passed and we have no idea what is going on.

To be honest, this is not what we call good cooperation, we actually work for you, so we ask you to give us minimal respect.

We understand that bureaucracy and administration takes it's time, but we think it should be doable in 1-3 weeks.

And we aren't slowing down on purpose as a political move, right?

So we would like to see progress and a publication this week.

Thank you very much, we nevertheless hope for a good cooperation.

Best Regards

Anthony Schneiter aka. muffinx

Jannis Kirschner aka. xorkiwi

Updated by **level_1** 8 days ago

#12

Hello muffinx, xorkiwi

Thanks for your feedback.

We understand your frustration and are sorry about that.

However we can assure you that your submission is being taken very seriously and you will definitely be hearing from us in the upcoming days.

Thanks for your patience and understanding.

Best regards,

-- SCRT Team

Updated by **level_1** 6 days ago

#13

Status changed from **INVESTIGATING** to **ACCEPTED**

Hello,

Your submission has been investigated and we are pleased to announce you that it has been ACCEPTED in the "BEST PRACTICES" category.

A brief summary of the vulnerability will be published today on the PIT platform (<https://www.onlinevote-pit.ch/stats/>).

You are free to publish your own report or communication about this issue.

Swiss Post have awarded you a CHF 400.- compensation. In order for the payment to be processed, we need to collect the following information:

- First name
- Last name
- Full Address
- Bank name
- Bank address
- Name of account Holder
- Account number
- Clearing
- BIC
- Amount

Congratulations and thanks for your patience.

Best regards,

-- SCRT Team

Updated by **muffinx** 6 days ago

#14

Dear SCRT Team

Thank you very much!

I will provide you the information needed for the payment ASAP.

Best Regards

Anthony Schneiter aka. muffinx

Jannis Kirschner aka. xorkiwi