Closed Opened 1 week ago by muffinx

General Unauthenticated REST Endpoints: Secure-Data-Manager Leak Admin Configuration

Dear E-Voting PIT Team

Now generally we noticed, that there is no authentication at all implemented in the Jax-RS REST endpoints, now this could potentially be explained that most values passed to the REST backends is complex data, like hashes and encrypted stuff.

Nevertheless this opens a range number of potential attack vectors. Even though there is a client-library and maybe not everything is accessible from outside, still it makes some stuff way simpler.

An example can be found in the Secure-Data-Manager:

/source-code/online-voting-secure-data-manager/secure-data-manager-backend/sdm-ws-rest/src/main/java/com/scytl/products/ov/sdm/ui/ws/rs/application/PreconfigurationResource.java

```
@RequestMapping(method = RequestMethod.POST, produces = "application/json")
@ResponseStatus(value = HttpStatus.CREATED)
@ApiOperation(value = "Get configuration", notes = "Service to retrieve the configuration of administration"
    + " boards and election events.", response = String.class)
public String createElectionEvent() throws IOException {

    transactionInfoProvider.generate(tenantId, "", "");

    secureLogger.log(Level.INFO, new LogContent.LogContentBuilder()
            .logEvent(SdmSecureLogEvent.SDM_SYNCHRONIZING_WITH_AP)
            .createLogInfo());

    String result = null;
    if (!isAdminPortalEnabled) {

        LOGGER.info(
                "The application is configured to not have connectivity to Admin Portal, " +
                        "check if this is the expected behavior");

        secureLogger.log(Level.ERROR,
                new LogContent.LogContentBuilder()
                        .logEvent(SdmSecureLogEvent.SDM_SYNCHRONIZATION_WITH_AP_FAILED)
                        .additionalInfo("err_desc",
                                "The application is configured to not have connectivity to Admin Portal, " +
                                "check if this is the expected behavior")
                        .createLogInfo());
    }
    // call to end point to download data from administration portal
    else if (preconfigurationRepository.download(configFile)) {
        // process the download data
        result = preconfigurationRepository.readFromFileAndSave(configFile);
    }

    secureLogger.log(Level.INFO, new LogContent.LogContentBuilder()
            .logEvent(SdmSecureLogEvent.SDM_SYNCHRONIZED_WITH_AP_SUCCESSFULLY)
            .createLogInfo());

    return result;
}
```

Now first it is checked if the admin portal is enabled, which is true by default:

```
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/sdm-ws-rest/sdmConfig/admin
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-service
```

Except here:

```
evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/sdm-db-utils/src/main/resou
```

Nevertheless, there is no authentication, so an attacker can easily send a POST request to

```
/sdm-ws-rest/preconfiguration
```

to recieve the admin configuration.

This is only the beginning, the code is really big and we're working hard. One could argument that these endpoints aren't (maybe?) not callable in the PIT? We don't know to be honest.

Still we want to report this, since this can be used in so many other possible attacks like SSRF, xss, malware and more..

Especially now where basically everyone has the source code.

Thank you very much for reading my report.

Best Regards

Anthony Schneiter aka. muffinx Jannis Kirschner aka. xorkiwi

Swisspost @swisspost added In Progress topic: general labels 1 week ago

Swisspost @swisspost · 1 week ago Maintainer

Hello Anthony,

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

Kind regards

muffinx @muffinx · 1 week ago Guest

Here is another one:

evoting-solution-master/source-code/online-voting-secure-data-manager/secure-data-manager-backend/sdm-ws-rest/src/main/java/com/scytl/products/ov/sdm/ui/ws/rs/application/SdmConfigResource.java

```
    @Autowired
private SdmConfigService sdmConfigService;

@RequestMapping(method = RequestMethod.GET , produces = "application/json")
@ApiOperation(value = "Get SDM configuration service", notes = "", response = String.class)
@ApiResponses({@ApiResponse(code = 500, message = "Internal Server Error")})
public ResponseEntity<?> getSdmConfig() {
    SdmConfigData config = new SdmConfigData();
    try {
        config.setConfig(sdmConfigService.getConfig());
    } catch (IOException e) {
            LOGGER.error ("Error trying to get SDM configuration.", e);
        return ResponseEntity.status(HttpStatus.INTERNAL_SERVER_ERROR).body(e.getMessage());
    }
    return ResponseEntity.ok(config);
}
```

Swisspost @swisspost · 1 week ago Maintainer

Hello Anthony,

Thank you again for your observations. Please note that the SecureDataManager is a component used for generating the voting cards and decryption (see also chapter 4.3.3 of the Scytl sVote Software Architecture document). It is not available over the internet and not active during the voting phase. The endpoints that the sdm-ws-rest backend exposes are the endpoints that are called by the front end (User Interface). Authentication between frontend and backend has been omitted since it is a standalone application and an attacker would need physical access to the SDM machine. If the attacker has this level of access to the machine, then is not reasonable to execute such attack, as the attacker is able to execute anything on the machine without the need of hacking the communication between the SDM components. Therefore, an additional authentication layer would not add any value

Kind regards

Swisspost @swisspost closed 1 week ago

muffinx @muffinx reopened 1 week ago

muffinx @muffinx closed 1 week ago

muffinx @muffinx · 1 week ago Guest

Dear E-Voting PIT Team

Thanks for you answers.

Now we have a pretty serious question, we don't want to get into arguing but we need to ask this.

If your saying, like in this issue that the SDM machine is just physical accessible and you said that sdm-ws-rest backend exposes stuff to the frontend.

Does that now mean that there is partial access or none at all?

Because we currently don't understand why the SDM is part of the PIT if it doesn't matter anyway. We want to know this so we can better plan our strategy for the PIT.

We already spent a lot of time on getting a general overview, doing basic analysis but now we are way more "focused" and we are quickly adapting our strategy.

Thank you very much for answering our issue.

Best Regards

Anthony Schneiter aka. muffinx Jannis Kirschner aka. xorkiwi

muffinx @muffinx reopened 1 week ago

Swisspost @swisspost · 1 week ago Maintainer

Hello you two,

We will try and sum up the whole infrastructure for you. Maybe the system documentation from Post can give you a little insight: https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting?shortcut=evoting -> under Transparency and publications -> E-Voting system documentation.

We will get back to you.

Kind regards

muffinx @muffinx · 1 week ago Guest

Dear E-Voting Team

Yes, a sum-up would be good. Thanks for the documentation, that already helped us understand more parts of the application.

Nevertheless we are pretty confused. In the PIT details there is writen (https://www.onlinevote-pit.ch/details/):

```
The scope of the PIT includes the public-facing service as well as corresponding e-voting backend of this dedi
cated instance:

pit.evoting-test.ch (Voter Access used by voters)
pit-admin.evoting-test.ch (Admin Access used by Secure Data Manager SDM)
```

And there is the SDM in it. Now please answer this question:

If it is not available on the internet (and this is the main argument against attacks of all sorts on the SDM), why include it in the PIT?

Because in our opinion it is a valid attack vector if you can just use certain Endpoints without an authentication.

Excuse us for our confusion(s).

Thank you very much for helping us.

Best Regards

Anthony Schneiter aka. muffinx Jannis Kirschner aka. xorkiwi

Swisspost @swisspost · 1 week ago Maintainer

Hi you two,

The "Online" SDM, which communicates in the productive case from the canton to the infrastructure of post, is used before and after the PIT.

In Chapter 5.3 of the Code of Conduct (PIT) describes that attacks on the setup of the vote are out of scope. The reason for this is that these operations happen as previously explained in an offline environment on the cantons premises. Concretely this means that communication between the SDM frontend and SDM backend are not in scope, as they happen on the same offline machine. However, the SDM needs to communicate with e-voting server components that are hosted within the swiss post infrastructure (concretely via the endpoint pit-admin.evoting-test.ch). The server components are in scope of the PIT.

During the PIT no communication between the SDM and the server components will happen. Trying to explain this further, the chapter 3.1.2 (system documentation post) happens before the PIT. After this, the "Online" SDM is not used anymore during the PIT. The next time the "Online" SDM is used is in chapter 3.3.2 (system documentation post), which happens after the PIT.

In case you have a question don't hesitate.

Kind regards

Swisspost @swisspost closed 1 week ago

Swisspost @swisspost removed In Progress label 1 day ago

Swisspost @swisspost made the issue visible to everyone 1 day ago