Security Vulnerability Report

SE-2011-01 Issue #1

[Persistent CSS in web application's code]

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 (`http://foto.onet.pl`). Błąd związany jest z brakiem odpowiednich filtrów po stronie serwera WWW wykrywającego znaki specjalne języka HTML. Brak wspomnianych filtrów umożliwia przemycenie w nazwie albumu fotograficznego elementów języka HTML. W szczególności, możliwe jest użycie elementu `<script>` i krótkiej sekwencji komend języka JavaScript.

Security Explorations zweryfikowało, iż skrypt zlokalizowany pod adresem `http://foto.onet.pl/_x/foto/api.php3` dopuszcza maksymalnie 33 znaki (50 minus długość znacznika `<script>` i `</script>`), które mogą zostać wykorzystane do konstrukcji sekwencji języka JavaScript.

W najbardziej oczywistym scenariuszu ataku, ww. błąd umożliwia załączenie złośliwego kodu JavaScript za pośrednictwem znaczników `<script>` lub `<iframe>` i odwołującego się poprzez atrybut `src` do strony na której atakujący udostępnia skrypt eksploatujący błąd bezpieczeństwa w oprogramowaniu aplikacyjnym użytkownika (przeglądarka, plugin, obiekt ActiveX, itp.).

Zgłoszony błąd w połączeniu z innymi bledami bezpieczeństwa środowiska platformy cyfrowej telewizji satelitarnej N (błąd numer 2), umożliwił zakończoną sukcesem penetrację dekoderów satelitarnych tejże 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 "Album 1",
- 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 nazw albumu fotograficznego użytkownika odpowiednio na "`Album 1`" i "`Album`"
- `moje_albumy.html.loaded`
  zawartość strony `moje_albumy.html` widzianej z poziomu dekodera telewizji satelitarnej N, strona zawiera 1 album na liście użytkownika danego dekodera o nazwie "`Album 1`", adres strony to `https://cs.n.onet.pl/nportal/nFoto_v2/moje_albumy.html`

Błąd numer 1 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.