Security Vulnerability Report

SE-2011-01 Issue #3

[brute force attack against Onet Lajt]

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 Lajt (`http://n.lajt.pl`). Błąd związany jest z brakiem implementacji po stronie serwera WWW mechanizmów uniemożliwiających przeprowadzenie ataku typu *Brute Force* zmierzającego do odkrycia kodu PIN użytkownika przypisanego do danej umowy abonenckiej o świadczenie usług telewizji satelitarnej N.

Security Explorations zweryfikowało, że w celu odkrycia 4-cyfrowego kodu PIN danego użytkownika, wystarczy wysłać co najwyżej 10000 żądań HTTP do skryptu `http://n.lajt.pl/epg/nagrywanie_lista.html`.

W katalogu `test` znajdują sie strony HTML zwrócone przez wspomniany skrypt dla odpowiednio błędnej i poprawnej wartości kodu PIN.

Poniżej przedstawiamy wynika działania naszego oprogramowania, które w sposób automatyczny odnajduje wartość kodu PIN użytkownika określonej umowy abonenckiej:

```
c:\_PROJECTS\DTV>r xxxxxxxxxx

Nr umowy:    xxxxxxxxxx

PIN:         XXXX

Box serial: BZZBxxxxxxxxxxxxx
```

Znajomość kodu PIN użytkownika umożliwia między innymi:

- uzyskanie informacji o numerze seryjnym dekodera przypisanego do określonej umowy abonenckiej,
- dokonywanie zamówień filmów Video on Demand (VOD) z poziomu dekodera telewizji satelitarnej N i portalu `https://cs.n.onet.pl/`.

Błąd numer 3 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.