# Security Vulnerability Report

SE-2011-01 Issue #20

[information leak of billing information]

## 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 mechanizmu dystrybucji informacji o płatnościach do abonentów telewizji satelitarnej N. Dekodery tej platformy, posiadają wbudowaną funkcjonalność informującą użytkownika o otrzymaniu faktury za świadczone usługi. Funkcjonalność ta zbudowana jest w oparciu o informacje otrzymywane z satelity za pośrednictwem dedykowanego strumienia MPEG2. Wartość PID tego strumienia wskazywana jest przez własność `p.emmcarousel` dedykowanego serwisu. W przypadku programów telewizji satelitarnej N, PID ten ma wartość 0x0641. Serwisy, które zawierają informacje o wspomnianym PID są serwisami typu `DATA_BROADCAST` i maja oznaczenie rozpoczynające sie od `EMM Carousel`.

Dane przesyłane w strumieniu dedykowanym dla informacji o płatnościach mają format zgodny z formatem sekcji danych protokołu MPEG2. Sekcje te posiadają następujące parametry:

- identyfikator tablicy (`table_id`) wynosi 0x04,
- offset od którego zlokalizowany jest adres karty Conax bez uwzględnienia najmłodszego bajtu to 0x08,
- bajt pod offsetem 0x09 ma wartość 0x01,
- offset od którego zlokalizowane są dane o płatnościach to 0x0f.

Z uwagi na pominięcie najmłodszego bajtu adresu karty Conax w sekcji o płatnościach, każda z nich może zawierać informacje o 256 płatnościach.

Podstawowe dane o płatnościach są przesyłane w postaci skompresowanej algorytmem GZ. Po rozpakowaniu maja one postać pakietów danych tekstowych ujętych pomiędzy znacznikami `<IP>` oraz `</IP>`. Przykładowy pakiet danych pokazany został poniżej:

```
<IP v="2a" p="12425ee" s="xxxxxxxxxxx" c="12feb5f8f18" d="1300f6c1318"
h="0" f="2" g="4" r="10" a="58.00" t="125155d"
l="e7">xxxxxxxxxx|FV/354182/1105/P|2011-05-01|2011-05-31|2011-05-
13|218.00|-218.00|0.00|0.00|58.00|58.00|39 2000 0017 8999 0000 2513
9958|2011-05-20|2$2%%17.00%#3%%17.00%#17%%17.00%#16%%17.00%|91$91%%-10.00%
od 2011-05-01 do 2011-05-31|1|</IP>
```

Dane o płatnościach nadawane przez operatora telewizji N zawierają miedzy innymi informacje o numerze klienta, numerze faktury, wpłatach abonenta, wysokości sumy do zapłaty oraz numerze karty Conax danego abonenta. Zgłoszony problem bezpieczeństwa związany jest z możliwością uzyskania informacji o:

- płatnościach wszystkich abonentów telewizji N z danego okresu rozliczeniowego (potencjalnie wrażliwa informacja handlowa),
- numerach umowy i numerach kart Conax wszystkich abonentów (informacje potencjalnie ułatwiające inne ataki).

Security Explorations zaimplementowało w swoim kodzie Proof of Concept funkcjonalność umożliwiająca wyświetlanie informacji o płatnościach nadawanych przez operatora telewizji N. Poniżej zaprezentowany został fragment informacji otrzymanej w wyniku działania tego kodu:

| INVOICE NUMBER | FROM | TO | AGREEMENT # | CARD NUMBER | PLN |
|---|---|---|---|---|---|
| FV/645728/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 54.00 |
| FV/16828/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 68.00 |
| FV/580773/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 54.00 |
| FV/248678/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 68.00 |
| FV/325166/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 48.00 |
| FV/631371/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 48.00 |
| FV/374573/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 0.00 |
| FV/631677/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 48.00 |
| IFV/654704/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 0.00 |
| FV/778634/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 118.00 |
| FV/367554/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 0.00 |
| FV/432583/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 54.00 |
| FV/699133/1109/P | 2011-09-01 | 2011-09-30 | xxxxxxxxxx | xxxxxxxxxxx | 63.00 |
| FV/383198/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 58.00 |
| FV/9968/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxx | xxxxxxxxxxx | 99.00 |
| FV/375080/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 124.00 |
| FV/432599/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 113.00 |
| FV/427610/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 58.00 |
| FV/361974/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 118.00 |
| FV/727538/1109/P | 2011-09-01 | 2011-09-30 | xxxxxxxxxx | xxxxxxxxxxx | 68.00 |
| FV/428252/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 0.00 |
| FV/326334/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 83.00 |
| FV/243382/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 68.00 |
| FV/169727/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 68.00 |
| IFV/442894/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 0.00 |
| FV/473542/1108/P | 2011-08-01 | 2011-08-31 | xxxxxxxxxx | xxxxxxxxxxx | 68.00 |
| FV/537958/1109/P | 2011-09-01 | 2011-09-30 | xxxxxxxxxx | xxxxxxxxxxx | 107.00 |
| FV/266760/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 104.76 |
| FV/430381/1110/P | 2011-10-01 | 2011-10-31 | xxxxxxxxxx | xxxxxxxxxxx | 99.00 |

```
FV/282815/1110/P   | 2011-10-01 | 2011-10-31 | xxxxxxxxxx   | xxxxxxxxxxx  | 0.00
FV/759545/1109/P   | 2011-09-01 | 2011-09-30 | xxxxxxxxxx   | xxxxxxxxxxx  | 136.00
FV/697261/1109/P   | 2011-09-01 | 2011-09-30 | xxxxxxxxx    | xxxxxxxxxxx  | 510.44
FV/179148/1110/P   | 2011-10-01 | 2011-10-31 | xxxxxxxxx    | xxxxxxxxxxx  | 58.00
IFV/420274/1110/P  | 2011-10-01 | 2011-10-31 | xxxxxxxxxx   | xxxxxxxxxxx  | 0.00
FV/300256/1110/P   | 2011-10-01 | 2011-10-31 | xxxxxxxxxx   | xxxxxxxxxxx  | 135.96
FV/31294/1110/P    | 2011-10-01 | 2011-10-31 | xxxxxxxx     | xxxxxxxxxxx  | 120.00
```

Security Explorations zweryfikowało, że opisanym sposobem możliwe jest uzyskanie informacji o płatnościach dla około 820 tys. abonentów.

Błąd numer 20 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.