Security Vulnerability Report

SE-2011-01 Issue # 4

[insecure network configuration of https://cs.n.onet.pl/dev/]

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 konfiguracji portalu `https://cs.n.onet.pl`. Analiza stron serwisów udostępnianych za pośrednictwem adresu `https://cs.n.onet.pl/nportal` ujawniła obecność serwera wirtualnego dostępnego publicznie za pośrednictwem adresu `https://cs.n.onet.pl/dev`. Strona główna tego serwisu została załączona do tego raportu (plik `index.html`). Jej analiza wykazała obecność odnośników do następujących, w większości nieznanych serwisów związanych z platformą telewizji satelitarnej N:

```
https://cs.n.onet.pl/dev/eMagazyn/                    "eMagazyn test"
https://cs.n.onet.pl/dev/aaa/                         "Images"
https://cs.n.onet.pl/dev/FraTestInfo/                 "Faktura FAQ"
https://cs.n.onet.pl/dev/FraTestInfo/indeximg.html    "Faktura z img FAQ"
https://cs.n.onet.pl/dev/template.html                "Faktura"
https://cs.n.onet.pl/nportal/index.html?noredir       "Frontowy nPortal"
https://cs.n.onet.pl/nportal/index.html?noredir&test2 "1x Frontowy nPortal"
https://cs.n.onet.pl/dev/nRadio/                      "nRadio"
https://cs.n.onet.pl/dev/test.html                    "tablica SERVER"
https://cs.n.onet.pl/dev/nPoczta/                     "nPoczta"
https://cs.n.onet.pl/dev/boxnumber.html               "Box Number"
https://cs.n.onet.pl/dev/ntvnb/                       "bok debug"
https://cs.n.onet.pl/dev/___NBOK/                     "nBOK odblokowany"
https://cs.n.onet.pl/dev/nBokBOXfront/                "nBOK dev test"
https://cs.n.onet.pl/nportal/nFaq/                    "nFaq front"
https://cs.n.onet.pl/nportal/nBokBOX/                 "nBok front"
https://cs.n.onet.pl/nportal/nStrefa/                 "nStrefa front"
https://cs.n.onet.pl/nportal/nportaltest2/            "nportal test"
https://cs.n.onet.pl/dev/__________nbokbg/            "nbok bg"
https://cs.n.onet.pl/dev/nBokDEMO/nBokBOX/            "nbok ZASLEPKA"
https://cs.n.onet.pl/dev/_FRONT_/nFoto_v2/            "xF"
https://cs.n.onet.pl/dev/_FRONT_/nPogoda/             "xP"
https://cs.n.onet.pl/dev/_FRONT_/nSport/              "xS"
https://cs.n.onet.pl/dev/FotoBigger/                  "OnetFoto FHD"
https://cs.n.onet.pl/dev/nBokx/                       "nBokx"
```

```
https://cs. n.onet.pl/dev/nSportfront/                  "nSport DEV"
https://cs.n.onet.pl/dev/nFoto/                         "nFoto TEST"
https://cs.n.onet.pl/dev/nBokBOXfront/                  "nBok TEST"
https://cs.n.onet.pl/dev/nKeyboard/                     "Klawiatura"
https://cs.n.onet.pl/dev/nClock/                        "Zegarek"
https://cs.n.onet.pl/dev/nAdvert/                       "Fiat advert"
https://cs.n.onet.pl/dev/nBokBOXtest/                   "nbok test"
https://cs.n.onet.pl/dev/nAdvert/test.html              "8 scale test"
https://cs.n.onet.pl/dev/nAukcje/                       "Allegro_test"
https://cs.n.onet.pl/dev/nAukcjeBackup/                 "aukcje xlet"
https://cs.n.onet.pl/dev/nAukcjeTest/                   "aukcje test"
https://cs.n.onet.pl/dev/nBokBOXfront/                  "nbok debug test"
https://cs.n.onet.pl/dev/nFoto/                         "foto"
https://cs.n.onet.pl/dev/nTvn24movie/                   "nTvn24"
https://cs.n.onet.pl/dev/ntvn245/                       "ntvn245"
https://cs.n.onet.pl/dev/nOnetTV/                       "nOnetTV"
https://cs.n.onet.pl/dev/VideoTestVod/convertTest/      "test"
https://cs.n.onet.pl/dev/__testowe/nPlejada/            "plejada"
https://cs.n.onet.pl/dev/VideoTestVod/urszula800/       "Urszula 800"
```

Powyższe odnośniki i ich nazwy jednoznacznie wskazują na to, że adres `https://cs.n.onet.pl/dev/` stanowi portal developerski, na którym udostępniane są wersje testowe wielu istniejących lub nowo opracowywanych aplikacji związanych ze środowiskiem dekoderów platformy N. Ze względów bezpieczeństwa, tego typu portale nie powinny być jednak dostępne publicznie.

Strona główna portalu developerskiego zawierała również wiele informacji o konfiguracji serwera i jego zmiennych środowiskowych. Zostało to zilustrowane w załączonym pliku `config.txt`. Tego typu informacje mówią wiele o konfiguracji serwera proxy i środowisku sieciowym w jakim pracuje serwer WWW. Bardzo często stanowią również punkt odniesienia dla potencjalnych intruzów, pragnących uzyskać dostęp do sieci wewnętrznej danej korporacji (w tym przypadku Onet.pl S.A.).

Błąd numer 4 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.