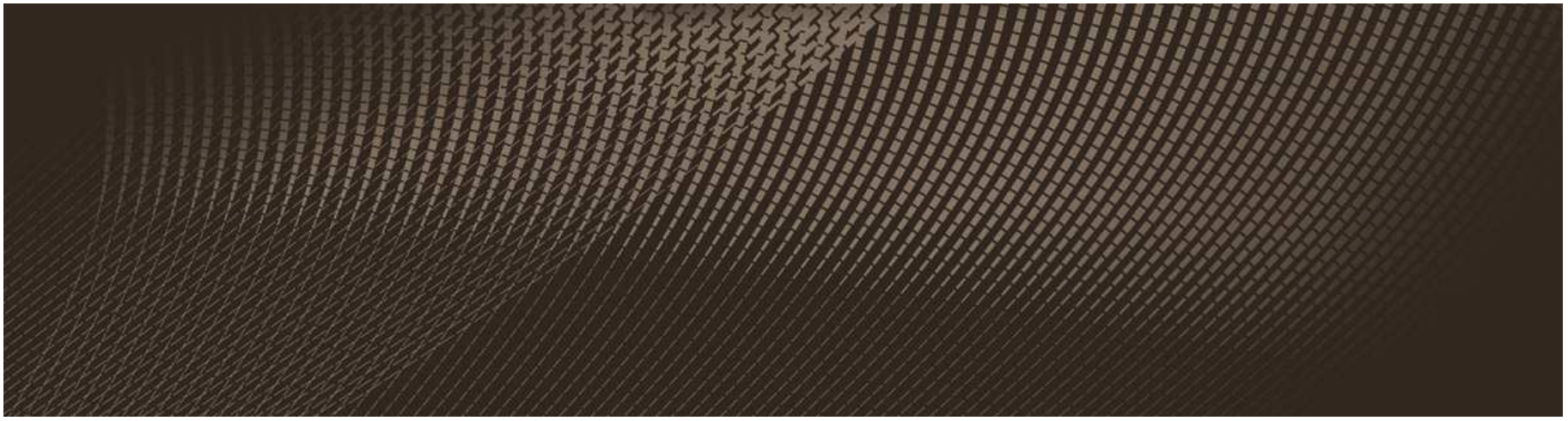


Sikkerhet i flash

OWASP-møte

Torsdag 04.02.2010 – Erlend Oftedal

BEKK

Adobe Flash

- Kjører som regel som en plugin i browseren
- Brukes til:
  - Reklame
  - Bannere
  - Spill
  - Video
  - Osv.

Flash

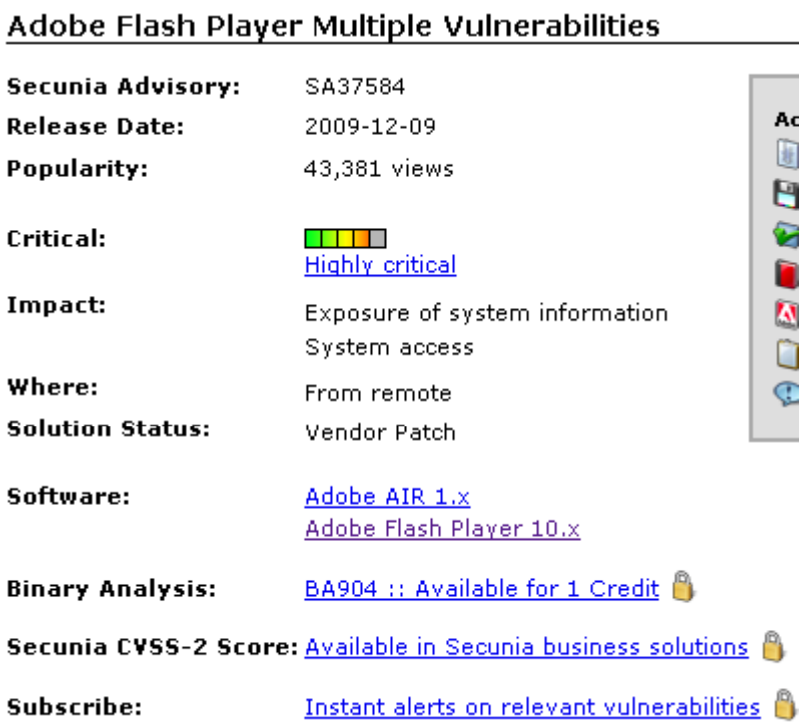
- Lastes ned og installeres
  - Direkte fra Adobe
  - Via en tjeneste som kjører på datamaskinen etter installasjon
- Lastes via <embed> eller <object>-tagger i HTML
- Det er blitt mer vanlig å laste via javascript en direkte via HTML

Flash som filformat

- Kalles ofte for en film (movie)
- Kode og brukergrensesnitt lages som regel i verktøy fra Adobe
- Kode skrives i ActionScript
  - Minner litt om javascript
  - Er sterkt typet
- Kompileres ned til .swf (uttales ofte ”sviff”)
  - Formatet er godt dokumentert
  - Kan dekompileres (kommer tilbake til dette)
  - Består av bytecode som tolkes av flash-plugin

Adobe - plugin

- Har en noe brokete fortid:
  - 73 registrerte feil i CVE
- Med andre ord viktig å oppdatere ofte



Adobe Flash Player Multiple Vulnerabilities

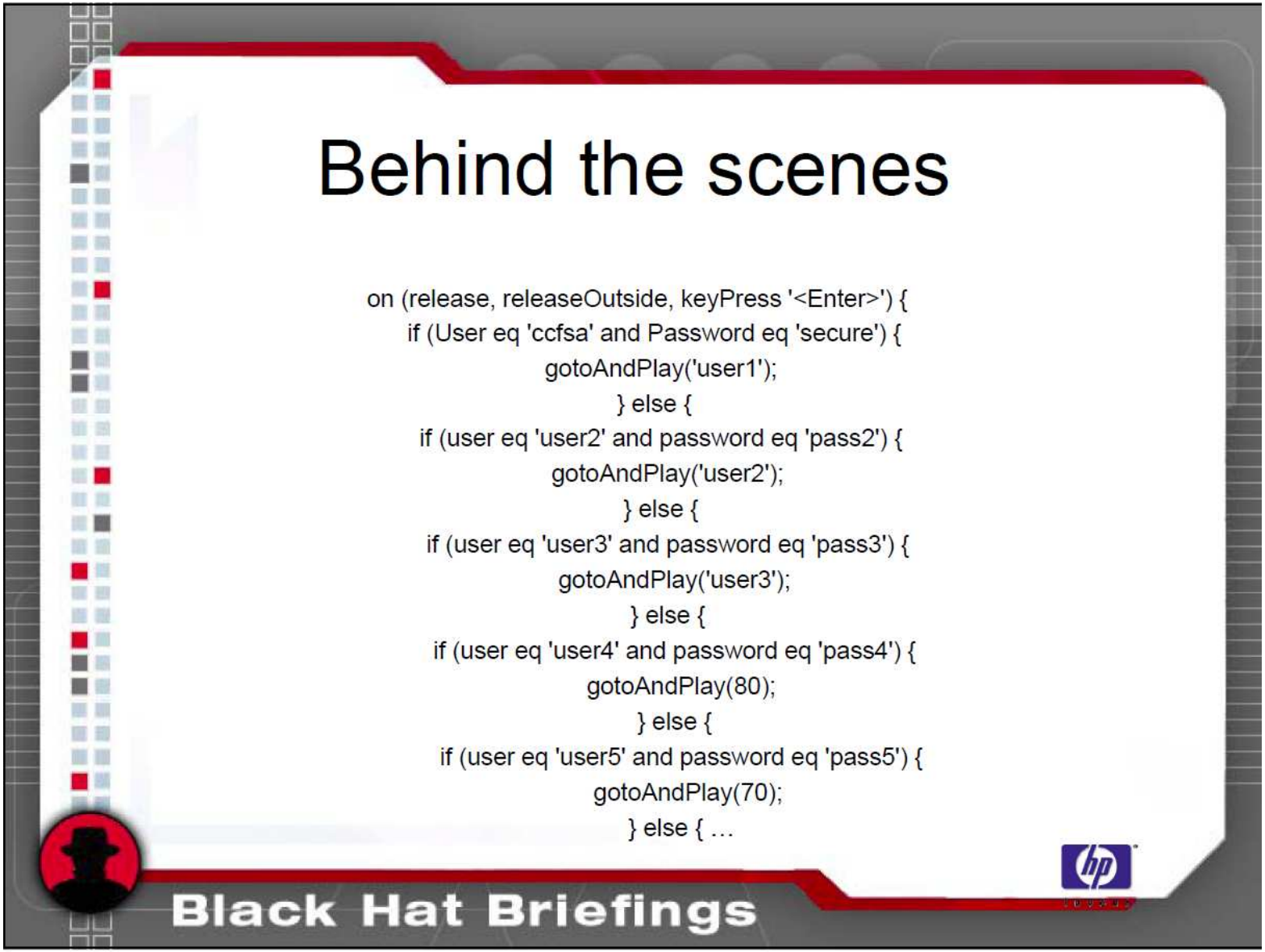
Secunia Advisory:	SA37584
Release Date:	2009-12-09
Popularity:	43,381 views
Critical:	Highly critical
Impact:	Exposure of system information System access
Where:	From remote
Solution Status:	Vendor Patch
Software:	Adobe AIR 1.x Adobe Flash Player 10.x
Binary Analysis:	BA904 :: Available for 1 Credit
Secunia CVSS-2 Score:	Available in Secunia business solutions
Subscribe:	Instant alerts on relevant vulnerabilities

Flash vs. Apple

- Apple dropper flash-støtte i iPad
- Men hadde flash-støtte i noen av iPad-videoene

Dekompilering av flash

”Blinded by Flash” – Prajakta Jagdale



Dekompilering av flash

- Flasm - http://flasm.sourceforge.net/
  - Dekomplierer flash til en flash-variant av assembly
  - Kan rekompilere en flash etter endringer

Dekompilering av flash

- Flare - http://www.nowrap.de/flare.html
  - Dekompilerer flash til actionscript

Dekompilering av flash

- HP SwfScan
  - Dekompilerer flash til actionscript
    - Noe styggere output enn Flare
  - Skal også kunne scanne etter sikkertsfeil

Hva med koden?

- Flash utvikles ofte av designere med lav eller ingen programmeringskunnskaper
- Flash kompileres til et program som kan ta input
- Flash-filer mangler som regel inputvalidering

Media

XSS vulnerability in Flash 8 million files

22:40 18.12.2009

Continue the theme that I raised in 2008 in his article XSS vulnerability 215,000 in flash files. Then I found hundreds of thousands of usb flash drives vulnerable to Cross-Site Scripting attacks. After the previous article, published 12.11.2008, I continued to study and found that more usb flash drives - millions of flash files - vulnerable to XSS attacks. How to usb flash drives in various global and local banner systems and usb flash drives at some sites.

XSS vulnerability in the 34 million Flash files

22:44 09.01.2010

In December, in his article XSS vulnerability in Flash 8 million files, I wrote that the Internet is to 34,000,000 usb flash drives tagcloud.swf potentially vulnerable to XSS attacks. Vrahovuchy that few paid attention to in the previous article in my memory about another 34 million vulnerable usb flash drives, I decided to write about a separate article.

Cross Site-Scripting (XSS)

- Sårbare funksjoner som navigateTo og getURL kan utnyttes til å kjøre javascript – URL-format:

  javascript:alert(”xss”)

XSS i TextField

- Kan utnyttes på samme måte som getURL og navigateToURL
  - `<img src='javascript:code//.jpg'>`
  - `<img src='asfunction:function, arg .jpg'>`
- Eksempel:

```
this.createTextField("txtBranchAddress",
 this.getNextHighestDepth(), 10, 10, 200, 200);
txtBranchAddress.html = true;
txtBranchAddress.htmlText = _root.branch;
```

- Angrep:

```
http://host/contact.swf?branch=<img src='asfunction:getURL,
javascript:alert("XSS") .jpg'>
```

Hva med Cross Site Request Forgery? (XSRF)

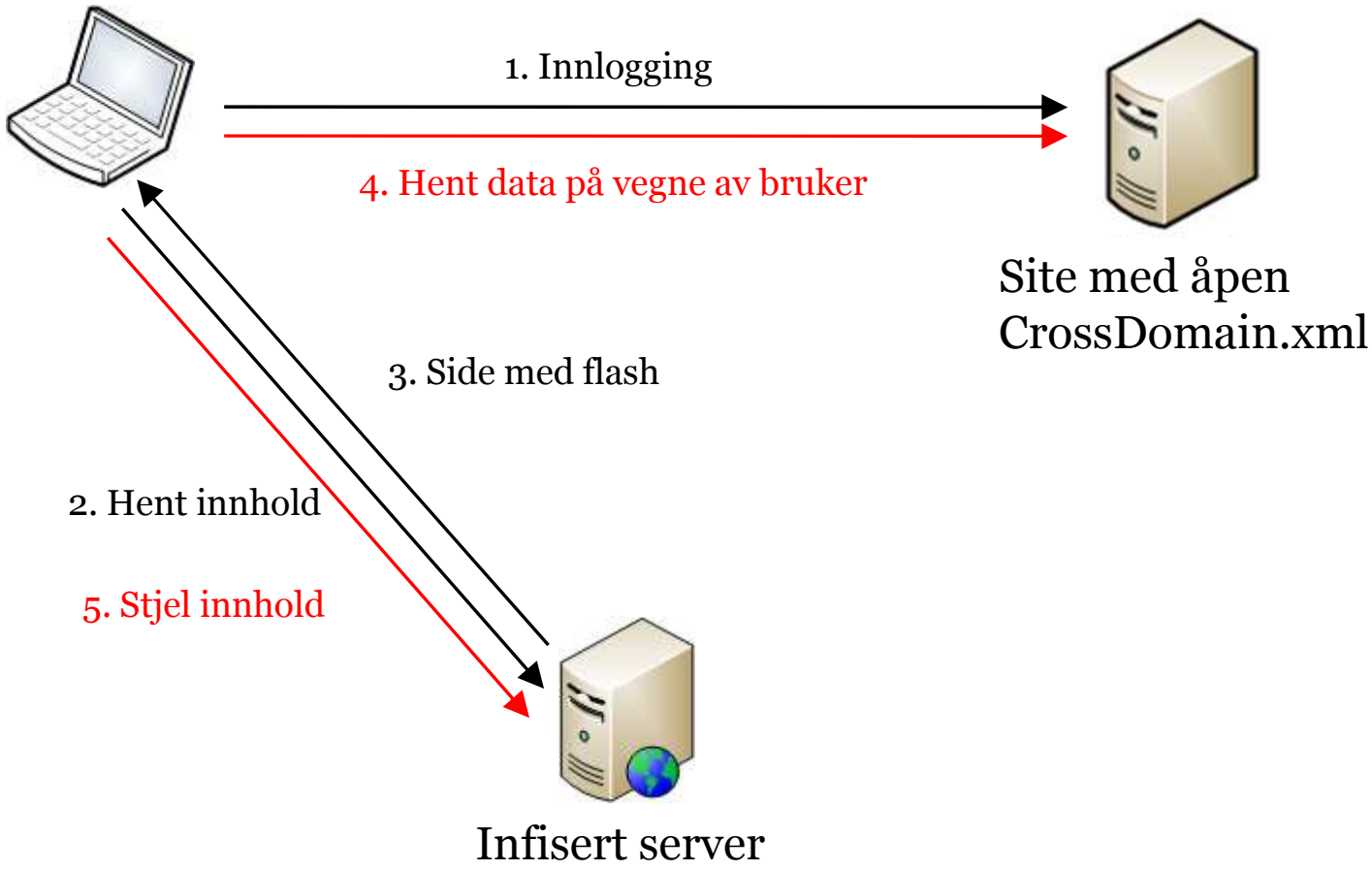
CrossDomain.xml

- Sier om en flash/flex applikasjon kan koble seg til et domene for å lese data
- Ofte alt for åpen:

```
<cross-domain-policy>
   <allow-access-from domain="*"/>
</cross-domain-policy>
```

- Kan utnyttes i et XSRF-angrep

XSRF mot åpen CrossDomain.xml



XSRF-angrep mot åpen CrossDomain.xml

- Site A har en åpen CrossDomain.xml og tilbyr i tillegg kundespesifikke sensitive data på URL http://A/xyz. Denne URLen krever pålogging.

- Angriper lager en flex/flash app som henter senitive data fra http://A/xyz og legger den på sin side http://B/attack.swf
- Angriper lurer en bruker til å besøke http://B/ som blant annet laster flashen
- Siden forspørslene i flashen gjøres fra browser og på vegne av brukeren, kan flashen lese sensitive data
- Flashen sender data til angriper

Sikker CrossDomain.xml

- CrossDomain.xml kan defineres på katalognivå
- Dermed kan man åpne for alle domener bare for gitte URLer

Videre lesning

- http://www.blackhat.com/presentations/bh-dc-09/Jagdale/BlackHat-DC-09-Jagdale-Blinded-by-Flash.pdf
- http://www.adobe.com/devnet/flashplayer/articles/secure_swf_apps.html

Spørsmål?