SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Cíl útoku: uživatel

Michal Tresner

AEC, spol. s r.o.

Trendy útoků posledních let

Krádeže strukturovaných dat

- **emaily,**
- **čísla karet**
- **hesla**

Krádeže nestrukturovaných dat

- **citlivé dokumenty,**
- **obchodní tajemství,**
- **finanční výkazy,**
- **průmyslové vzory**
- **a další.**

- **Zpeněžovány jsou informace, ne jen data**
  - **prodej informací tisku, médiím, zájmovým skupinám, zpeněžení na burze**
- **Malware je velmi komplexní a jeho detailní analýza se stává časově i finančně neúnosnou**
- **Malware je vytvářen organizovanými skupinami lidí (vládou sponzorované organizace, teroristické skupiny, cyber gangy)**

APT - Advanced Persistent Threat

- **Advanced** — použití pokročilých technik a nástrojů
- **Persistent** — dlouhotrvající útok, obtížně odhalitelné
- **Threat** — hrozba (existuje záměr i schopnosti)

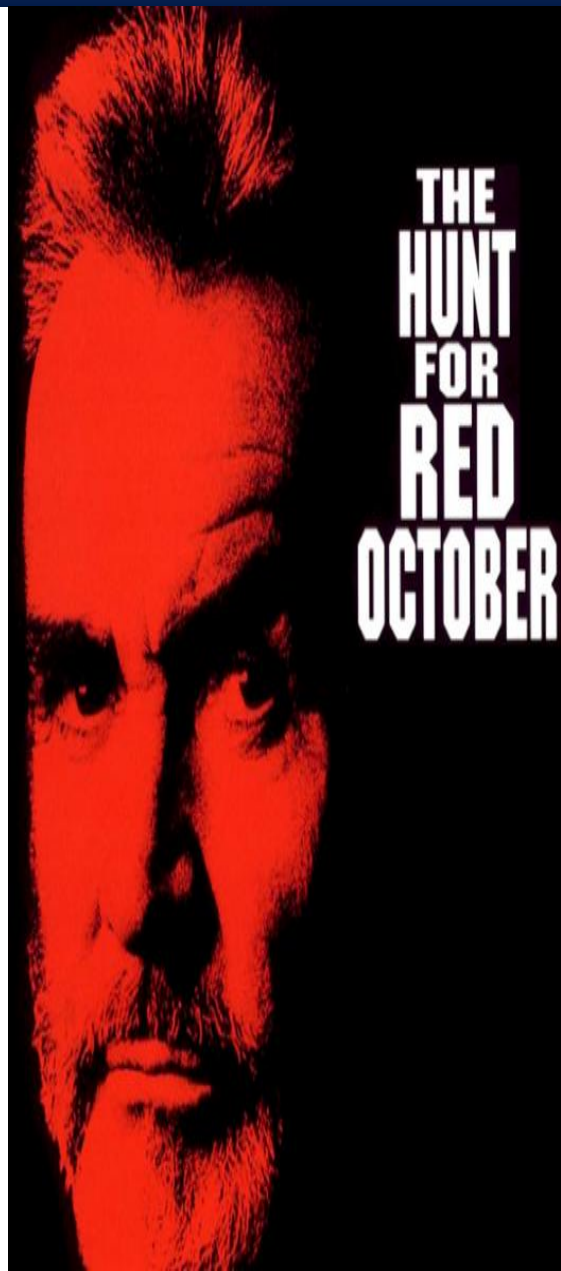
Zdroj: secureworks.com

Největší (nejznámější) APT útoky posledních let

- **Operation Aurora (2009) – technologické, zbrojní a bezpečnostní korporace napadeny 0-day chybou v IE**
- **Stuxnet (2010) – sabotážní malware útočící na SCADA systémy Iranského jaderného programu**
- **Duqu (2011) – následovník Stuxnetu, napsaný v neznámém high-level jazyce**
- **Flame (2012) – modulární špionážní toolkit útočící na středním východě, extrémně rozsáhlý (20 MB)**
- **Gauss (2012) – pokročilý malware zaměřený na krádeže hesel a bankovních údajů na středním východě**
- **Red October (2012/13) – útok na vládní diplomacie, odhalen po 5 letech aktivního působení**

Další nespecifikované útoky pocházející z Číny:

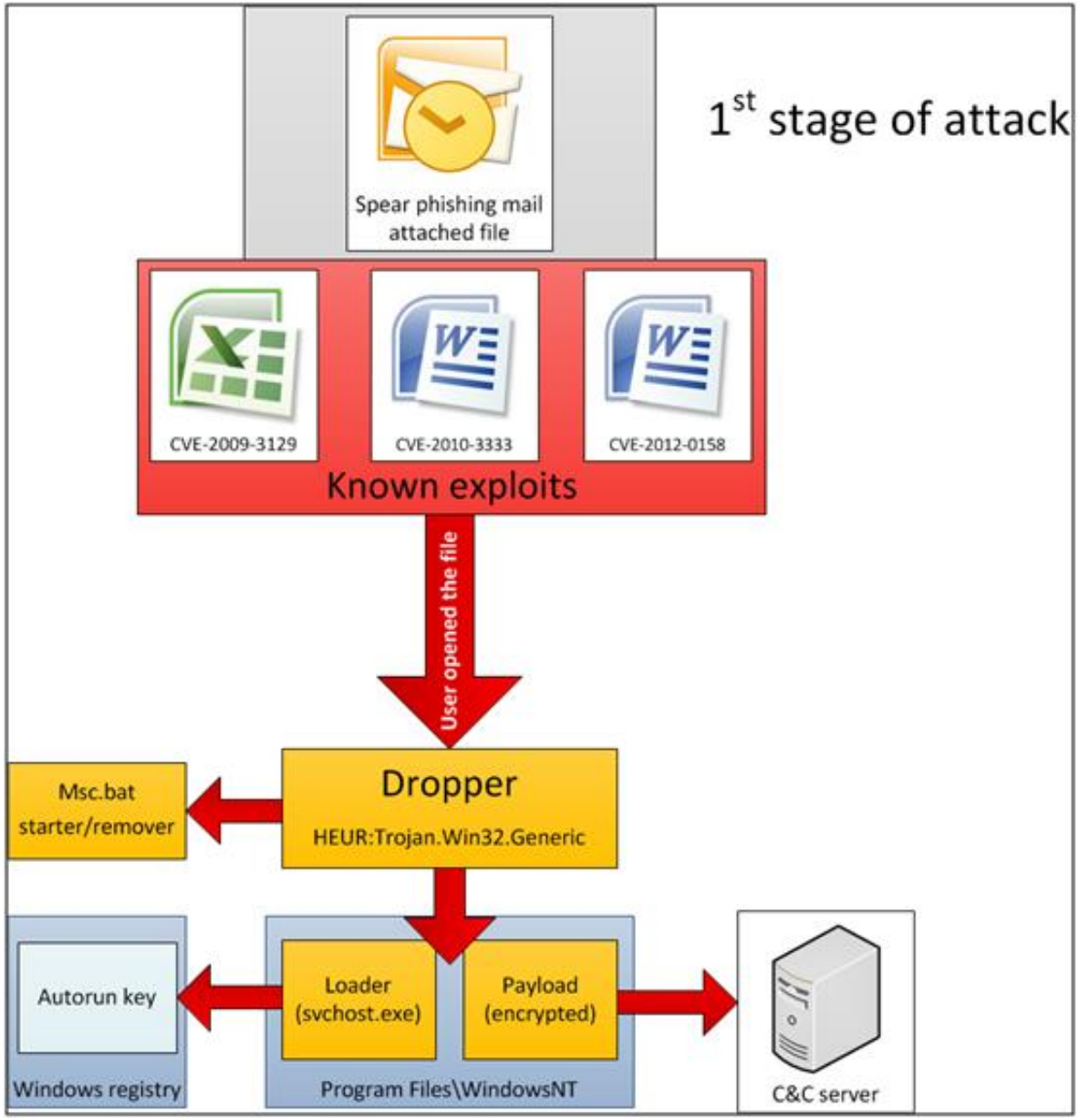
- **Wall Street Journal, New York Times**
- **Twitter – 250 000 účtů resetováno**



Metody útoku

- Spear Phishing
- Bouncer List Phishing – útok pouze pro zvané
- Watering Hole Attack
- Infikovaná Media
- Server Hacking

Průběh útoku



Motivace útočníků pro útoky na klientský SW

- Servery jsou lépe chráněny (services, FW, …)
- Cílení na konkrétní osoby je snazší (email, IM, s. sítě)
- Útoky na klientský SW jsou efektivní (DEP, ASLR byp.)
- Skutečně citlivá data jsou nejčastěji uložena na klientských stanicích (kdo s kým a za kolik)

Nejčastěji zneužívaný klientský SW

- Prohlížeče
- Zásuvné moduly a rozšíření prohlížečů
- Univerzální runtime prostředí (Java, .NET)
- Balík MS Office
- Adobe Reader – PDF soubory

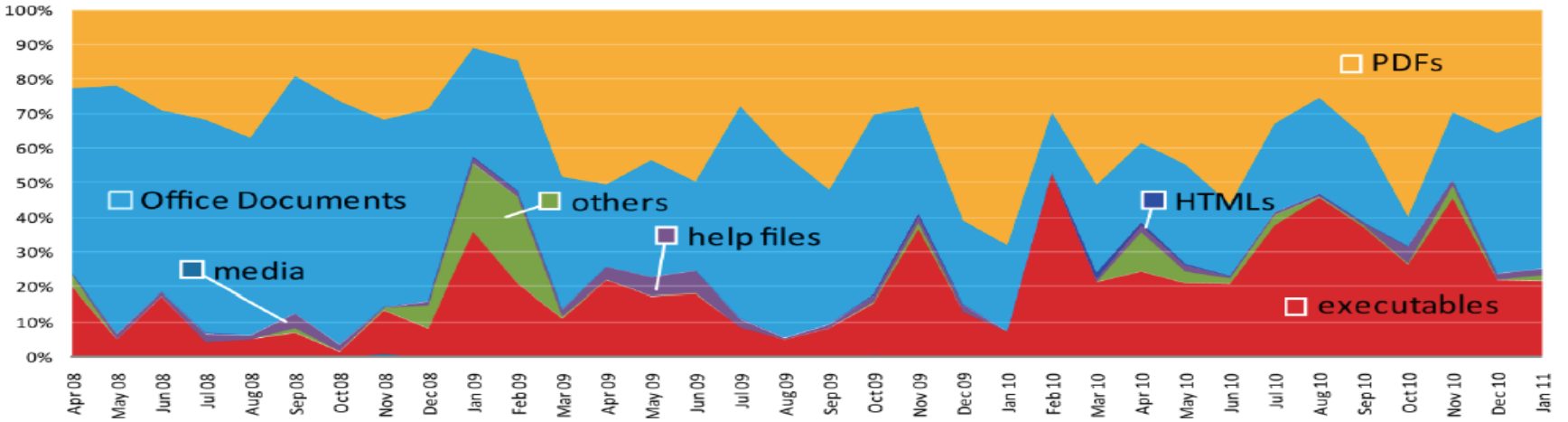
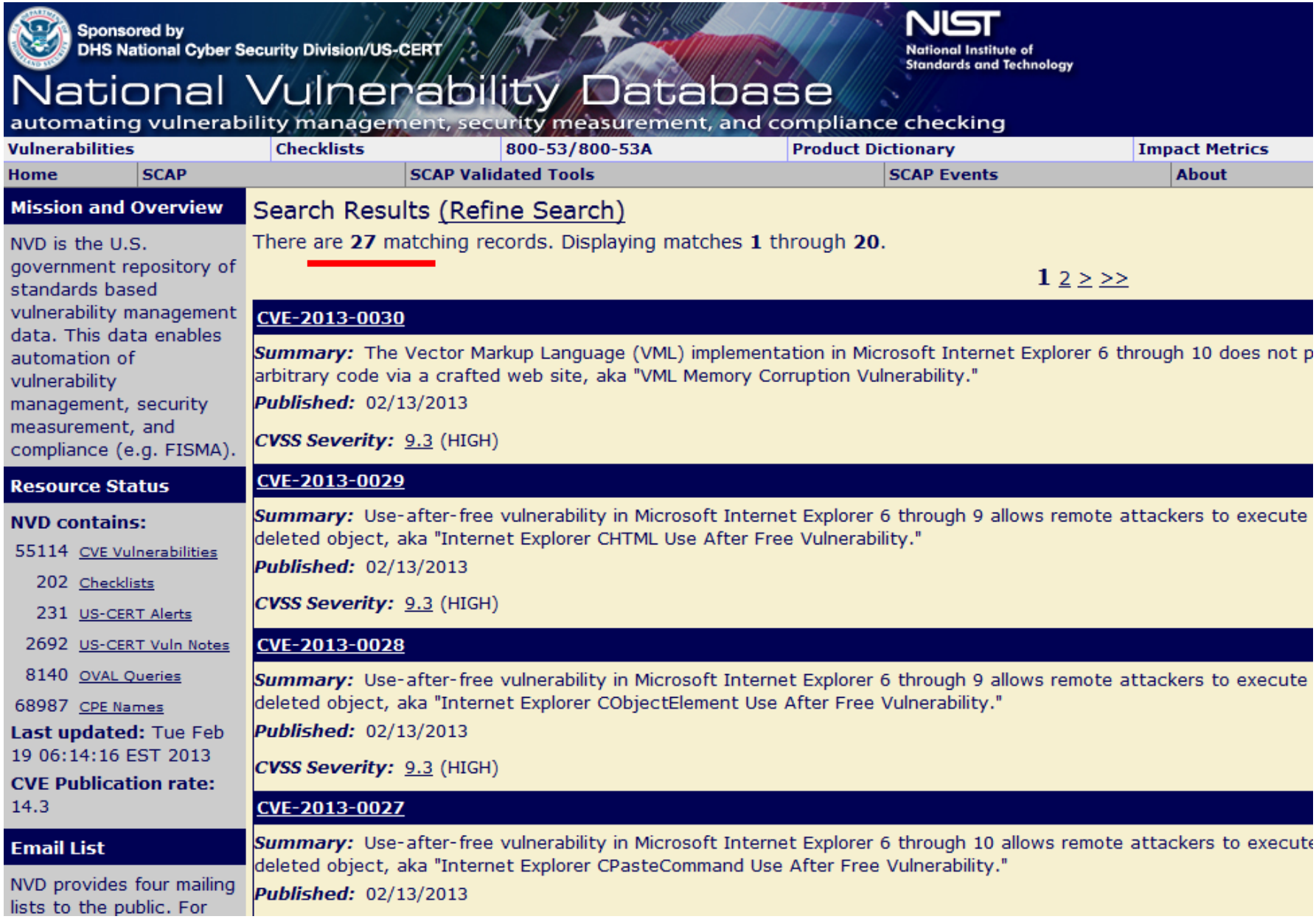


Figure 3 - Distribution of file types used over time

Zdroj: ZDNet

Internet Explorer (poslední 3 měsíce)



Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics

Home | SCAP | SCAP Validated Tools | SCAP Events | About

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

55114 CVE Vulnerabilities
202 Checklists
231 US-CERT Alerts
2692 US-CERT Vuln Notes
8140 OVAL Queries
68987 CPE Names

Last updated: Tue Feb 19 06:14:16 EST 2013

CVE Publication rate: 14.3

Email List

NVD provides four mailing lists to the public. For

Search Results (Refine Search)

There are **27** matching records. Displaying matches **1** through **20**.

1 2 > >>

CVE-2013-0030

Summary: The Vector Markup Language (VML) implementation in Microsoft Internet Explorer 6 through 10 does not p arbitrary code via a crafted web site, aka "VML Memory Corruption Vulnerability."

Published: 02/13/2013

CVSS Severity: 9.3 (HIGH)

CVE-2013-0029

Summary: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 9 allows remote attackers to execute deleted object, aka "Internet Explorer CHTML Use After Free Vulnerability."

Published: 02/13/2013

CVSS Severity: 9.3 (HIGH)

CVE-2013-0028

Summary: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 9 allows remote attackers to execute deleted object, aka "Internet Explorer CObjectElement Use After Free Vulnerability."

Published: 02/13/2013

CVSS Severity: 9.3 (HIGH)

CVE-2013-0027

Summary: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 10 allows remote attackers to execute deleted object, aka "Internet Explorer CPasteCommand Use After Free Vulnerability."

Published: 02/13/2013

Firefox (poslední 3 měsíce)

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics

Home | SCAP | SCAP Validated Tools | SCAP Events | About

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

55114 CVE Vulnerabilities
202 Checklists
231 US-CERT Alerts
2692 US-CERT Vuln Notes
8140 OVAL Queries
68987 CPE Names

Last updated: Tue Feb 19 06:14:16 EST 2013

CVE Publication rate: 14.3

Email List

NVD provides four mailing lists to the public. For

Search Results (Refine Search)

There are **60** matching records. Displaying matches **1** through **20**.

1 2 3 > >>

CVE-2013-1489

Summary: Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update Firefox, Opera, and Google Chrome, allows remote attackers to bypass the "Very High" security level of the Java Co user via unknown vectors, aka "Issue 53" and the "Java Security Slider" vulnerability.

Published: 01/31/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-0771

Summary: Heap-based buffer overflow in the gfxTextRun::ShrinkToLigatureBoundaries function in Mozilla Firefox be 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitra

Published: 01/13/2013

CVSS Severity: 9.3 (HIGH)

CVE-2013-0770

Summary: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Thunderbird befo cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown

Published: 01/13/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-0769

Summary: Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 10.x Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to or possibly execute arbitrary code via unknown vectors.

Chrome (poslední 3 měsíce)

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metri

Home | SCAP | SCAP Validated Tools | SCAP Events | About

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

55114 CVE Vulnerabilities
202 Checklists
231 US-CERT Alerts
2692 US-CERT Vuln Notes
8140 OVAL Queries
68987 CPE Names

Last updated: Tue Feb 19 06:14:16 EST 2013

CVE Publication rate: 14.3

Email List

NVD provides four mailing

Search Results (Refine Search)

There are **66** matching records. Displaying matches **1** through **20**.

1 2 3 4 > >>

CVE-2013-1489

Summary: Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Upd Firefox, Opera, and Google Chrome, allows remote attackers to bypass the "Very High" security level of the Java user via unknown vectors, aka "Issue 53" and the "Java Security Slider" vulnerability.

Published: 01/31/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-0843

Summary: content/renderer/media/webrtc_audio_renderer.cc in Google Chrome before 24.0.1312.56 on Mac O which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibl audio.

Published: 01/24/2013

CVSS Severity: 7.5 (HIGH)

CVE-2013-0842

Summary: Google Chrome before 24.0.1312.56 does not properly handle %00 characters in pathnames, which

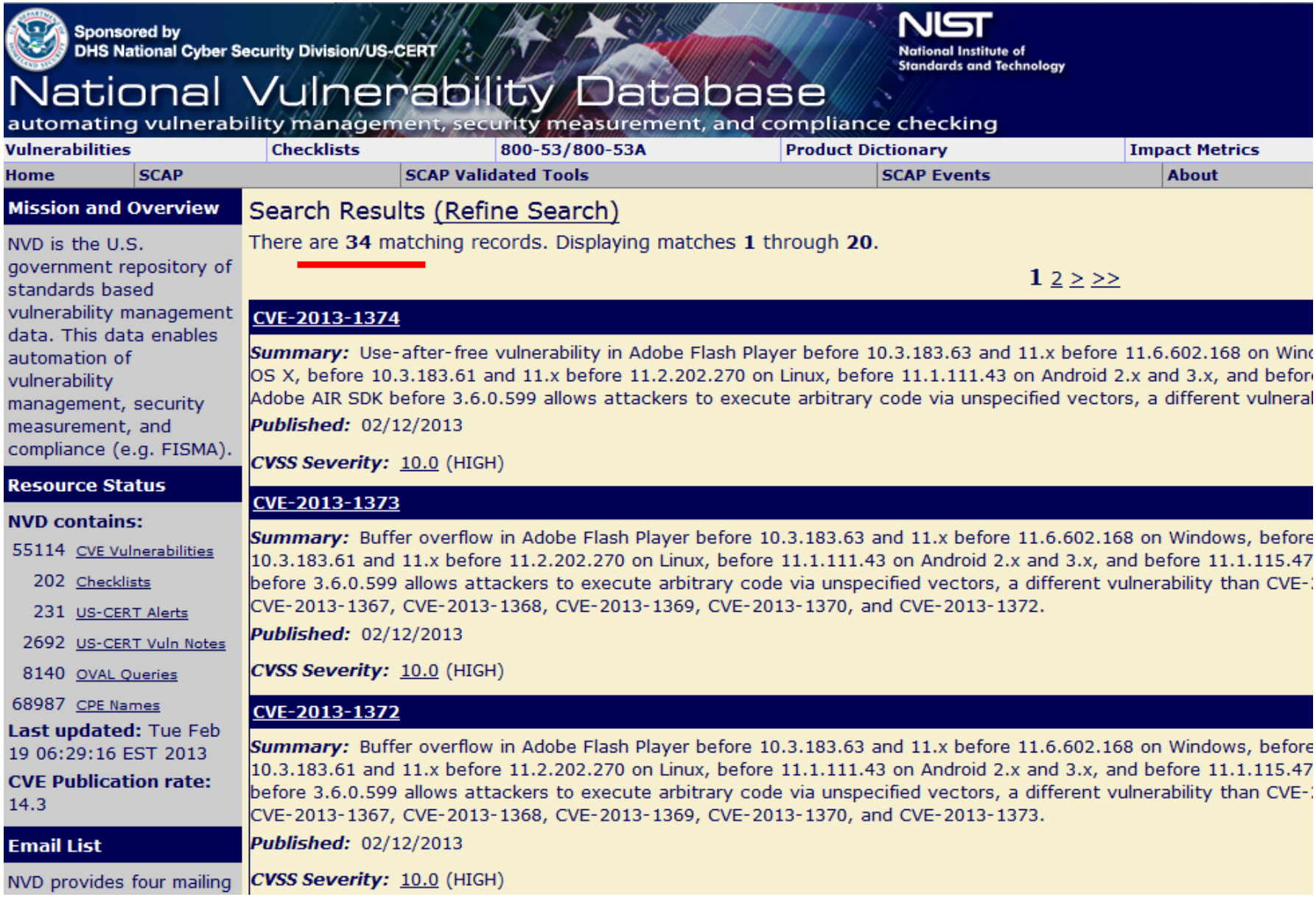
Published: 01/24/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-0841

Summary: Array index error in the content-blocking functionality in Google Chrome before 24.0.1312.56 allows unspecified other impact via unknown vectors.

Adobe Flash (poslední 3 měsíce)



Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics

Home | SCAP | SCAP Validated Tools | SCAP Events | About

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

55114 CVE Vulnerabilities
202 Checklists
231 US-CERT Alerts
2692 US-CERT Vuln Notes
8140 OVAL Queries
68987 CPE Names

Last updated: Tue Feb 19 06:29:16 EST 2013

CVE Publication rate: 14.3

Email List

NVD provides four mailing

Search Results (Refine Search)

There are **34** matching records. Displaying matches **1** through **20**.

1 2 > >>

CVE-2013-1374

Summary: Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability

Published: 02/12/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-1373

Summary: Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, and CVE-2013-1372.

Published: 02/12/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-1372

Summary: Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, and CVE-2013-1373.

Published: 02/12/2013

CVSS Severity: 10.0 (HIGH)

Java (poslední 3 měsíce)

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics

Home | SCAP | SCAP Validated Tools | SCAP Events | About

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

55114 CVE Vulnerabilities
202 Checklists
231 US-CERT Alerts
2692 US-CERT Vuln Notes
8140 OVAL Queries
68987 CPE Names

Last updated: Tue Feb 19 06:29:16 EST 2013

CVE Publication rate: 14.3

Email List

NVD provides four mailing lists to the public. For information and subscription instructions

Search Results (Refine Search)

There are **98** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 > >>

CVE-2013-1624

Summary: The TLS implementation in the Bouncy Castle Java library before 1.48 and C# library before 1.8 does not MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct dis analysis of timing data for crafted packets, a related issue to CVE-2013-0169.

Published: 02/08/2013

CVSS Severity: 4.0 (MEDIUM)

CVE-2013-1483

Summary: Unspecified vulnerability in the JavaFX component in Oracle Java SE JavaFX 2.2.4 and earlier allows rem unknown vectors, a different vulnerability than other CVEs listed in the February 2013 CPU.

Published: 02/02/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-1482

Summary: Unspecified vulnerability in the JavaFX component in Oracle Java SE JavaFX 2.2.4 and earlier allows rem unknown vectors, a different vulnerability than other CVEs listed in the February 2013 CPU.

Published: 02/02/2013

CVSS Severity: 10.0 (HIGH)

CVE-2013-1481

Summary: Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 6 through remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Sound.

Published: 02/02/2013

CVSS Severity: 10.0 (HIGH)

Vysvětlení pojmů

- **Exploit**

  je speciální program, data nebo sekvence příkazů, které využívají programátorskou chybu, která způsobí původně nezamýšlenou činnost software a umožňuje tak získat nějaký prospěch (ovládnutí počítače nebo nežádoucí instalaci software)

- **Payload**

  obsah dat přenášených v rámci útoku. Obvykle obsahuje samotné spustitelné tělo viru nebo jinak nebezpečného kódu

- **Shellcode**

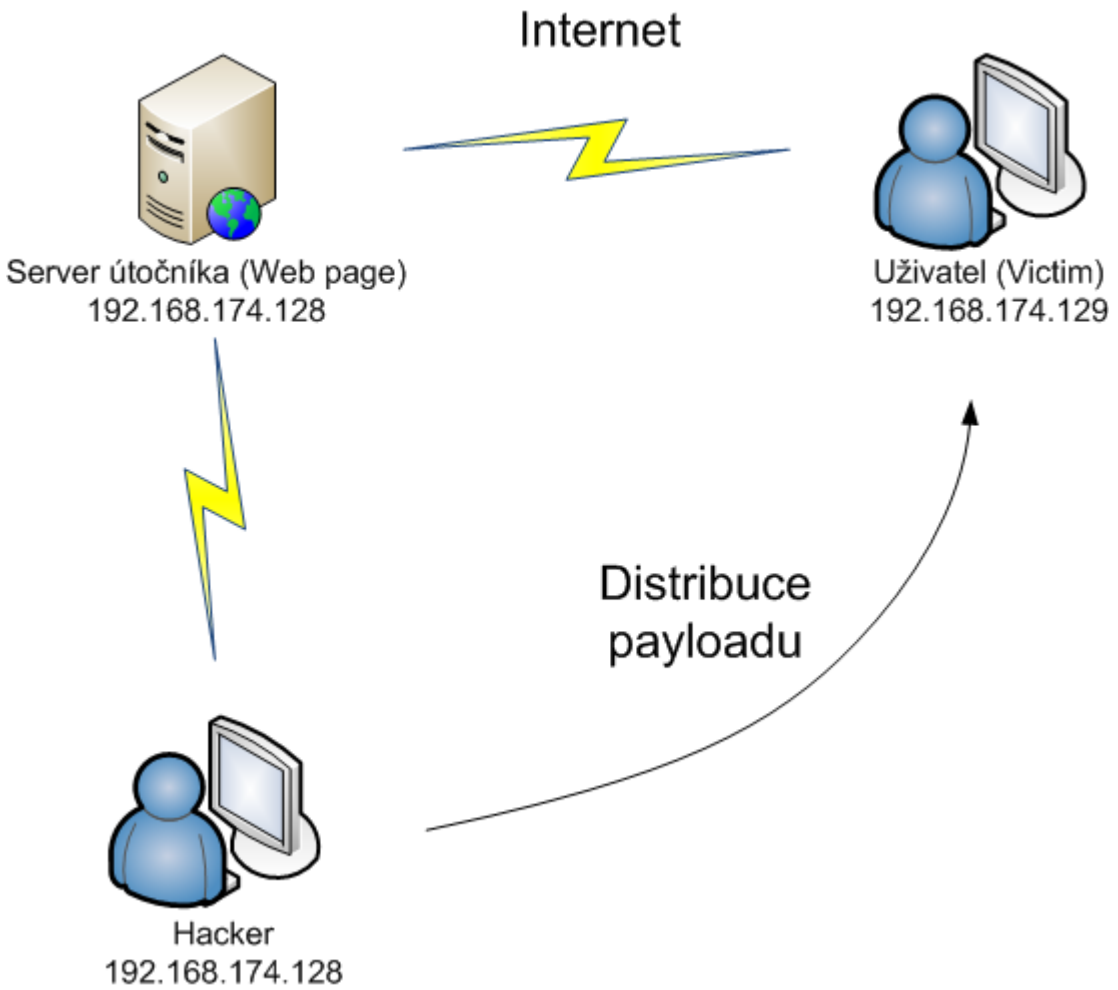
  část payloadu zodpovědná za otevření Shellu po úspěšném vykonání payloadu

- **Shell**

  Příkazový řádek systému, umožňuje interakci se systémem.

Ukázka – útok na uživatele

- **Testovací síť**



A co mobilní zařízení?

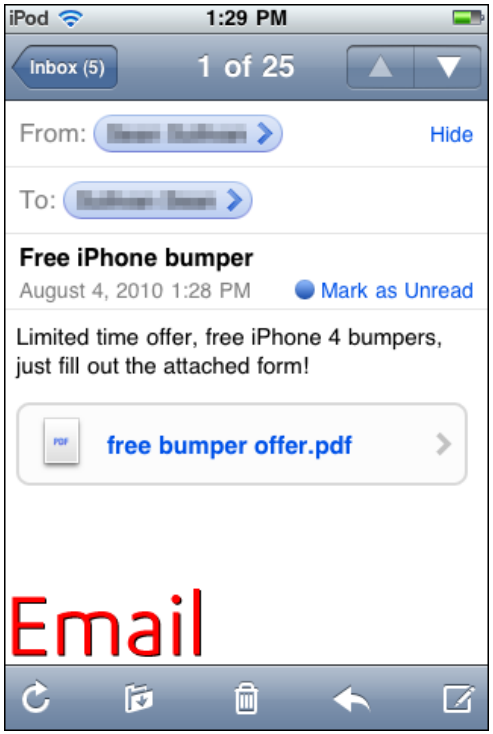
- Chytré mobilní telefony a tablety jsou vystaveny stejným problémům jako desktopy
- Počet nově objevených zranitelností se zvyšuje úměrně se zvyšováním počtu mobilních zařízení na trhu

Zajímavé příklady:

- Zeus trojan (multiplatformní mobilní malware) obchází dvoufaktorovou autentizaci u bankovních aplikací

- Samsung and HTC Android remote wipe USSD:

  <frame src="tel:*2767*3855%23" />



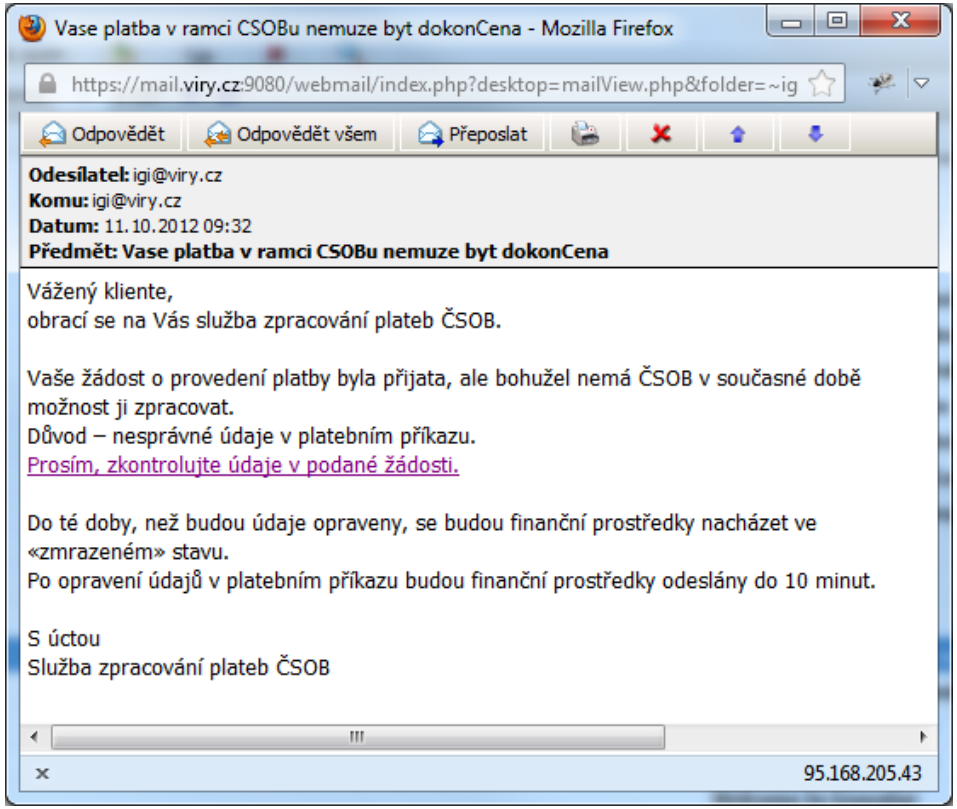
Jak se bránit?

Absolutní jistota neexistuje (0-day exploity)

Profesionální audit + penetrační test sítě výrazně snižuje riziko napadení

- **používat antivir**
- **používat neprivilegovaný účet**
- **nenavštěvovat nedůvěryhodné weby**
- **nepoužívat zbytečně mnoho pluginu**

- **chovat se obezřetně!**
- **AKTUALIZOVAT,**
- **AKTUALIZOVAT,**
- **AKTUALIZOVAT!**



Kam dál?

Zdroje informací

- **http://www.metasploit.com/**
- **https://www.trustedsec.com/downloads/social-engineer-toolkit/**
- **http://www.oldapps.com/**

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Michal Tresner

AEC, spol. s r.o.

michal.tresner@aec.cz