

Najboljša varnost na svetu (ampak samo za IPv6!)

Jan Bervar

jan@nil.si



NIL ASSIST

NIL HYPER
center

VITEL 2010

Najboljše prakse varne vpeljave IPv6 v poslovna okolja IT

- Ali so grožnje v omrežjih IPv6 drugačne kot grožnje v omrežjih IPv4?
- Kako drugačne so ranljivosti samega protokola IPv6 nasproti protokolu IPv4?
- Kako protokol IPv6 vpliva na ranljivosti ostalih delov informacijsko-komunikacijskih sistemov?

VITEL 2010

Najboljše prakse varne vpeljave IPv6 v poslovna okolja IT

- Vse najboljše visokonivojske (tehnološke in procesne) prakse varovanja ostajajo iste
- Naredite inventar kontrol IPv4 in jih prenesite v IPv6
- Dodajte kontrole, specifične za IPv6 (ND, RA, kontrola tunelov)
- Dobite občutek za IPv6
- Prepoznavajte omejitve današnjih varnostnih kontrol v IPv6
- Imejte plan B – pri prevelikem tveganju na delih infrastrukture počakajte z migracijo

Ranljivosti IPv6

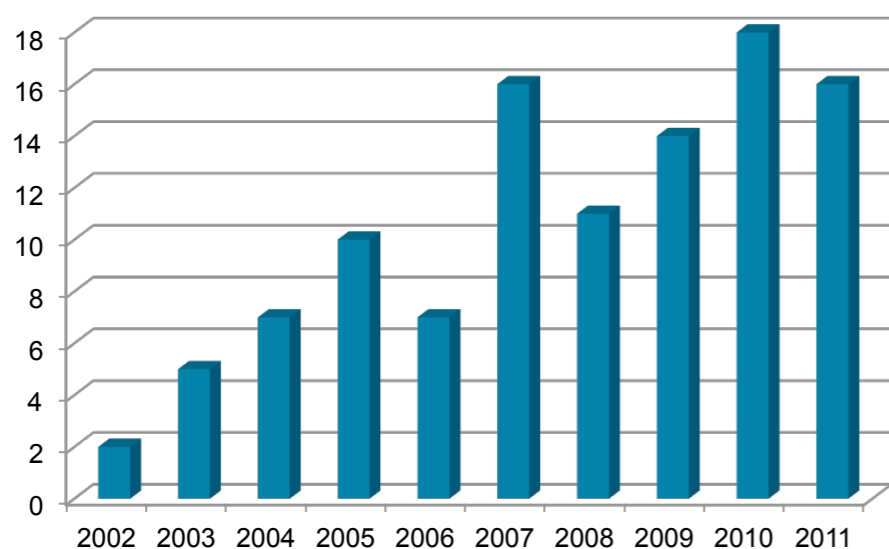
Nove stare ranljivosti

- Nepoznavanje tehnologije
- ND / RA / DHCPv6 napadi
- Izvorno usmerjanje
- Napadi na infrastrukturo (usmerjevalne protokol, kontrolno ravnino,...)
- **Implementacijske napake**

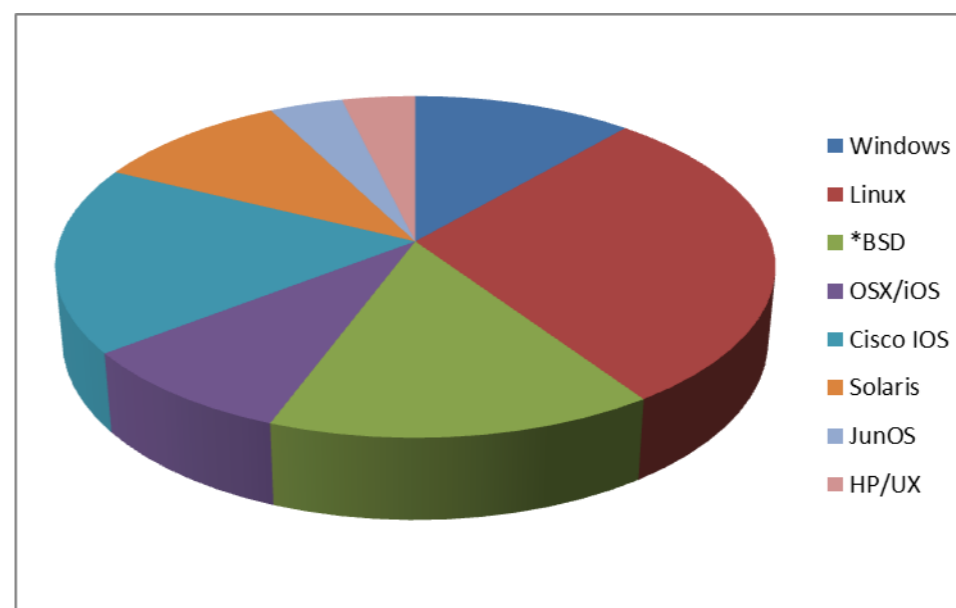
Nove ranljivosti

- Grožnje zasebnosti preko sledljivosti
- Nepričakovana povezljivost (tunelska in naravna!)

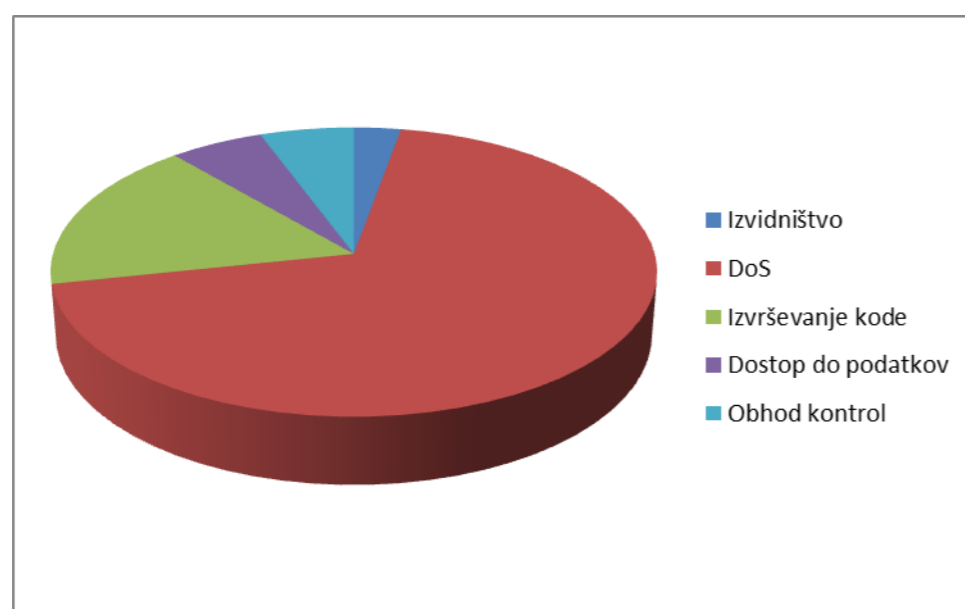
Implementacijske napake



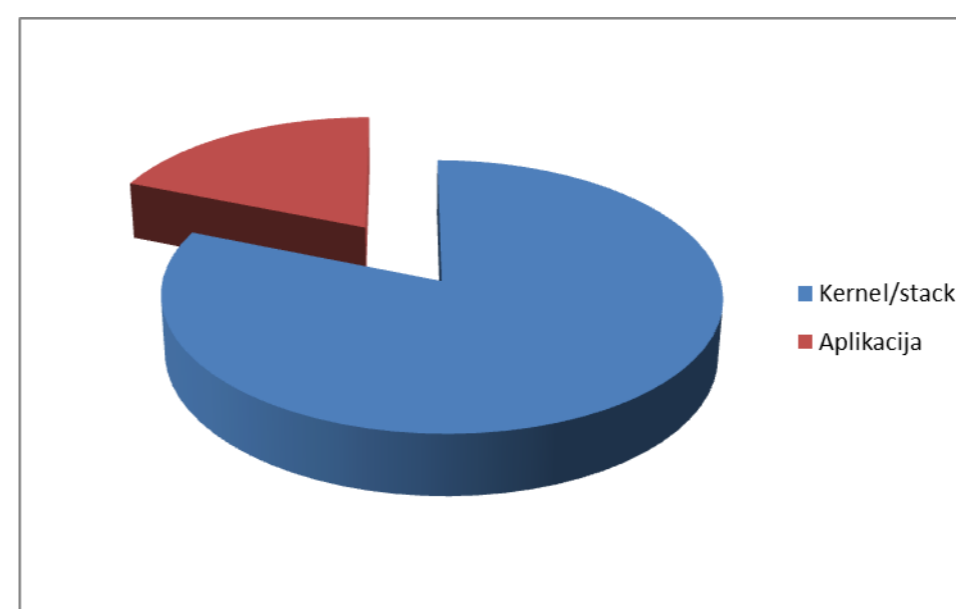
Število napak skozi leta



Napake glede na platformo

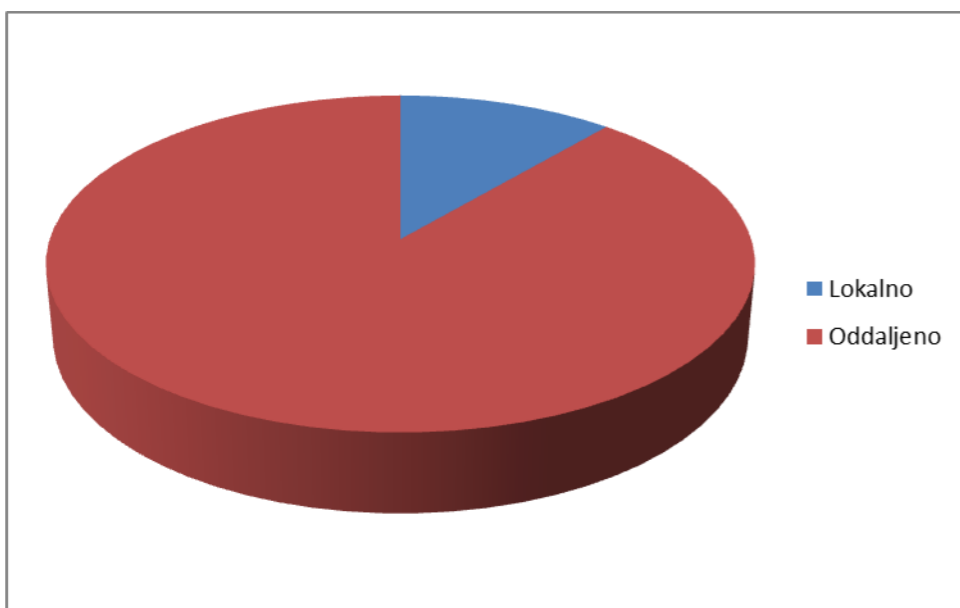


Napake glede na posledico

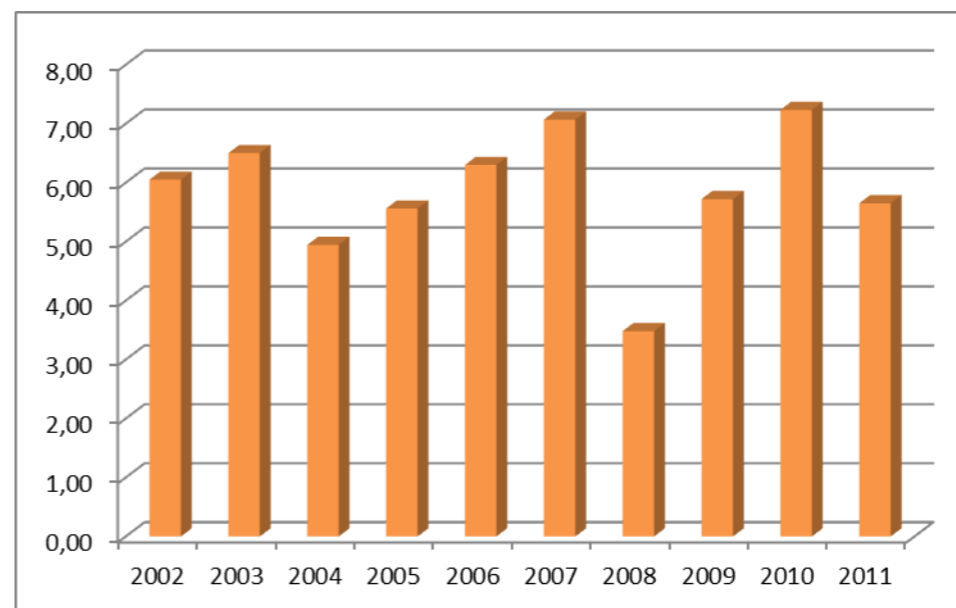


Napake glede na najdišče

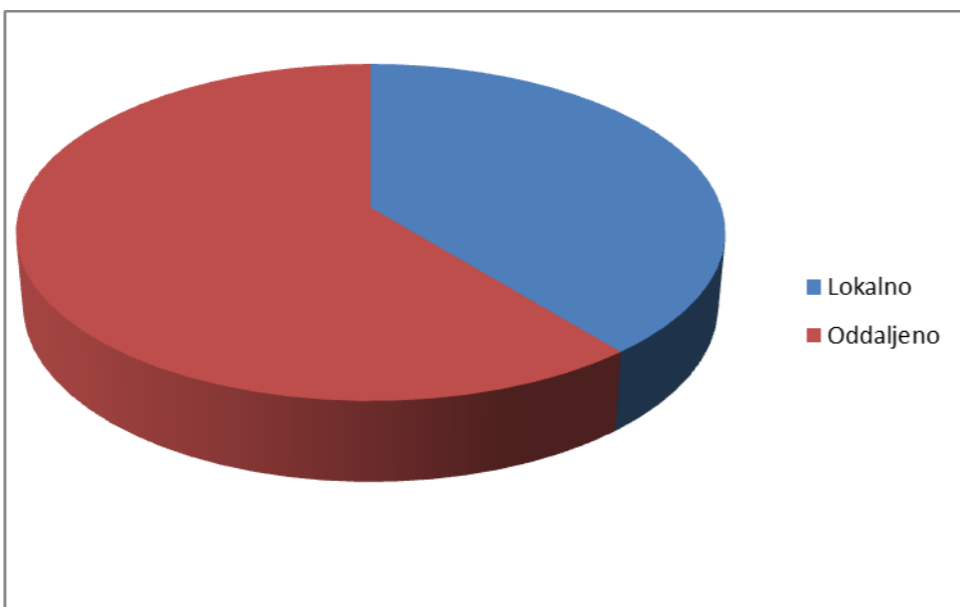
Implementacijske napake



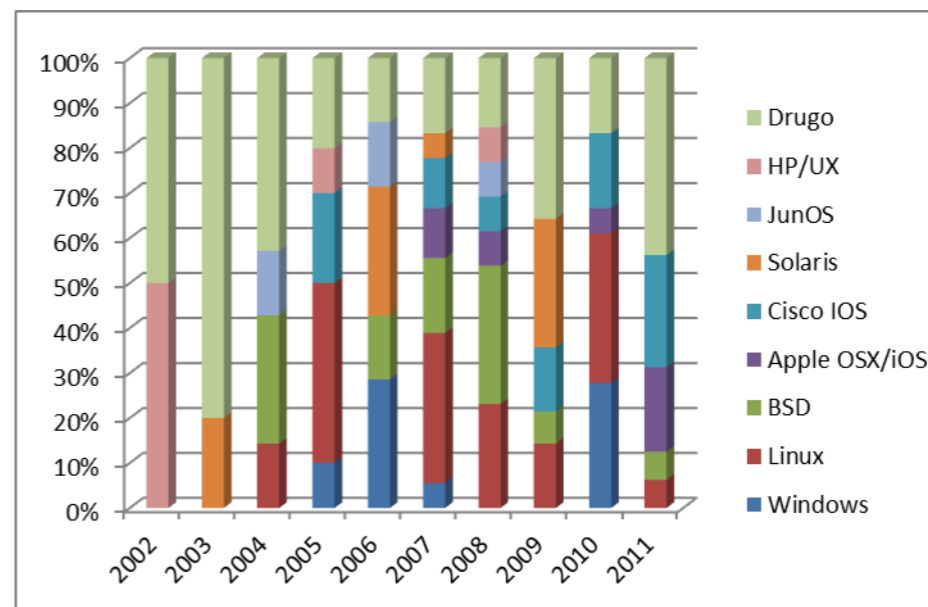
Napake glede na možnost napada



Povprečna resnost napak skozi leta



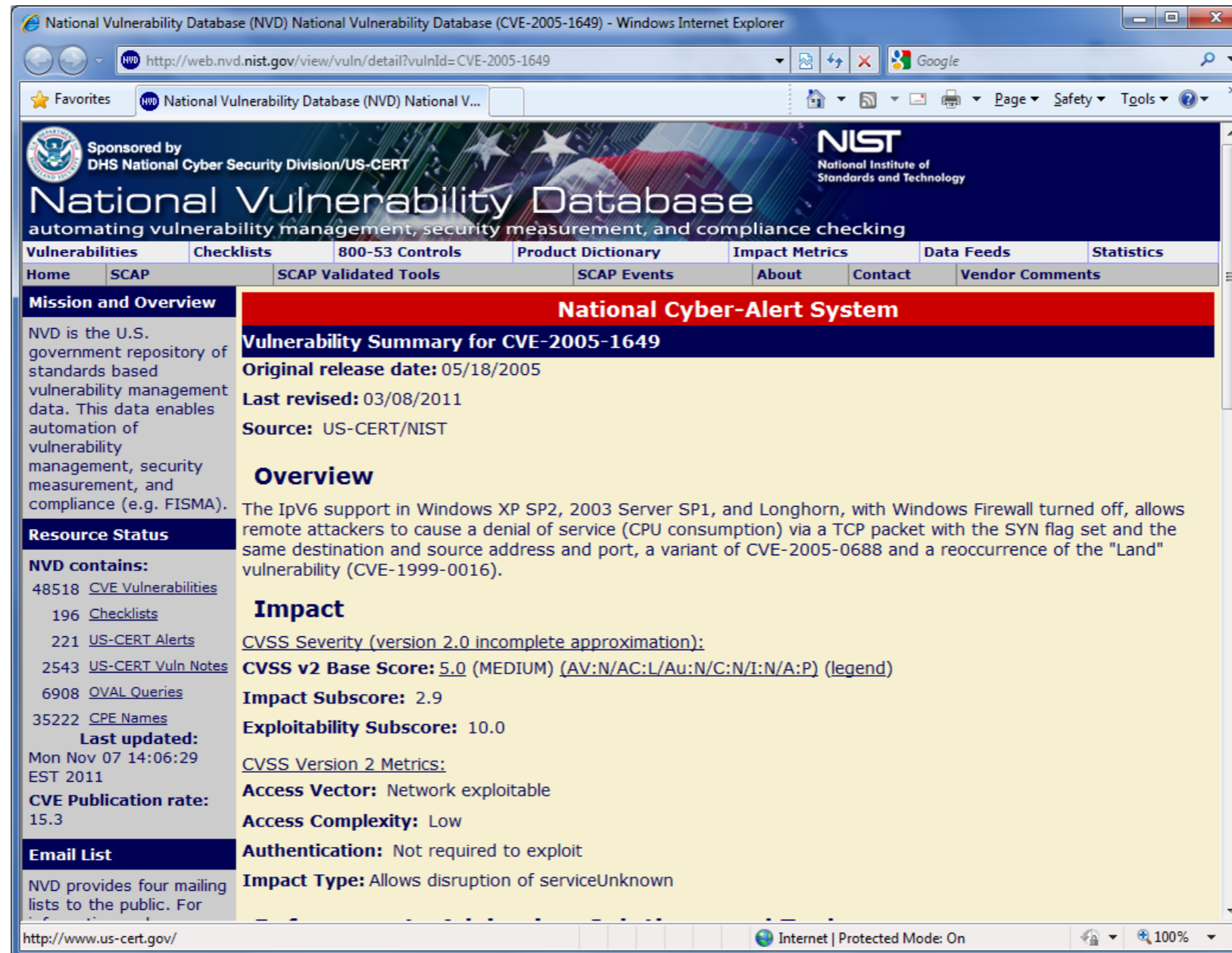
Napake glede na možnost napada (Linux)



Povprečna ranljivost platform skozi leta

Zanimivi primeri

Alien Resurrection



The screenshot shows the National Vulnerability Database (NVD) website in a Windows Internet Explorer browser. The page title is "National Vulnerability Database (NVD) National Vulnerability Database (CVE-2005-1649)". The URL is "http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1649".

The page is sponsored by the DHS National Cyber Security Division/US-CERT and NIST (National Institute of Standards and Technology). The main heading is "National Vulnerability Database" with the tagline "automating vulnerability management, security measurement, and compliance checking".

The navigation menu includes: Vulnerabilities, Checklists, 800-53 Controls, Product Dictionary, Impact Metrics, Data Feeds, and Statistics. The sub-menu includes: Home, SCAP, SCAP Validated Tools, SCAP Events, About, Contact, and Vendor Comments.

The main content area is titled "National Cyber-Alert System" and "Vulnerability Summary for CVE-2005-1649".

Original release date: 05/18/2005
Last revised: 03/08/2011
Source: US-CERT/NIST

Overview
 The IPv6 support in Windows XP SP2, 2003 Server SP1, and Longhorn, with Windows Firewall turned off, allows remote attackers to cause a denial of service (CPU consumption) via a TCP packet with the SYN flag set and the same destination and source address and port, a variant of CVE-2005-0688 and a reoccurrence of the "Land" vulnerability (CVE-1999-0016).

Impact
CVSS Severity (version 2.0 incomplete approximation):
CVSS v2 Base Score: 5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:N/A:P) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0
CVSS Version 2 Metrics:
Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows disruption of serviceUnknown

Resource Status
NVD contains:
 48518 [CVE Vulnerabilities](#)
 196 [Checklists](#)
 221 [US-CERT Alerts](#)
 2543 [US-CERT Vuln Notes](#)
 6908 [OVAL Queries](#)
 35222 [CPE Names](#)
Last updated:
 Mon Nov 07 14:06:29 EST 2011
CVE Publication rate:
 15.3

Email List
 NVD provides four mailing lists to the public. For

The footer shows "http://www.us-cert.gov/" and "Internet | Protected Mode: On".

Zanimivi primeri

Python Code Exec

The screenshot shows a Windows Internet Explorer browser window displaying the National Vulnerability Database (NVD) search results for CVE-2004-0150. The browser's address bar shows the URL: http://web.nvd.nist.gov/view/vuln/search-results?query=CVE-2004-0150&search_type=all&cves=o. The page header includes the NIST logo and the text "National Vulnerability Database automating vulnerability management, security measurement, and compliance checking". The page is sponsored by the DHS National Cyber Security Division/US-CERT. The search results section shows one matching record for CVE-2004-0150. The summary states: "Buffer overflow in the getaddrinfo function in Python 2.2 before 2.2.2, when IPv6 support is disabled, allows remote attackers to execute arbitrary code via an IPv6 address that is obtained using DNS." The vulnerability was published on 04/15/2004 and has a CVSS Severity of 7.5 (HIGH). The left sidebar contains navigation links for Mission and Overview, Resource Status, and Email List. The Resource Status section lists various data types and their counts, such as 48518 CVE Vulnerabilities and 196 Checklists. The last updated date is Mon Nov 07 14:21:29 EST 2011, and the CVE Publication rate is 15.3.

National Vulnerability Database (NVD) Search Vulnerabilities - Windows Internet Explorer

http://web.nvd.nist.gov/view/vuln/search-results?query=CVE-2004-0150&search_type=all&cves=o

alien resurrection

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 Controls Product Dictionary Impact Metrics Data Feeds Statistics

Home SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

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:

- 48518 [CVE Vulnerabilities](#)
- 196 [Checklists](#)
- 221 [US-CERT Alerts](#)
- 2543 [US-CERT Vuln Notes](#)
- 6908 [OVAL Queries](#)
- 35222 [CPE Names](#)

Last updated:
Mon Nov 07 14:21:29 EST 2011

CVE Publication rate:
15.3

Email List

NVD provides four mailing lists to the public. For

Search Results (Refine Search)

There is one matching record. Displaying match **1** of **1**.

CVE-2004-0150

Summary: Buffer overflow in the getaddrinfo function in Python 2.2 before 2.2.2, when IPv6 support is disabled, allows remote attackers to execute arbitrary code via an IPv6 address that is obtained using DNS.

Published: 04/15/2004

CVSS Severity: 7.5 (HIGH)

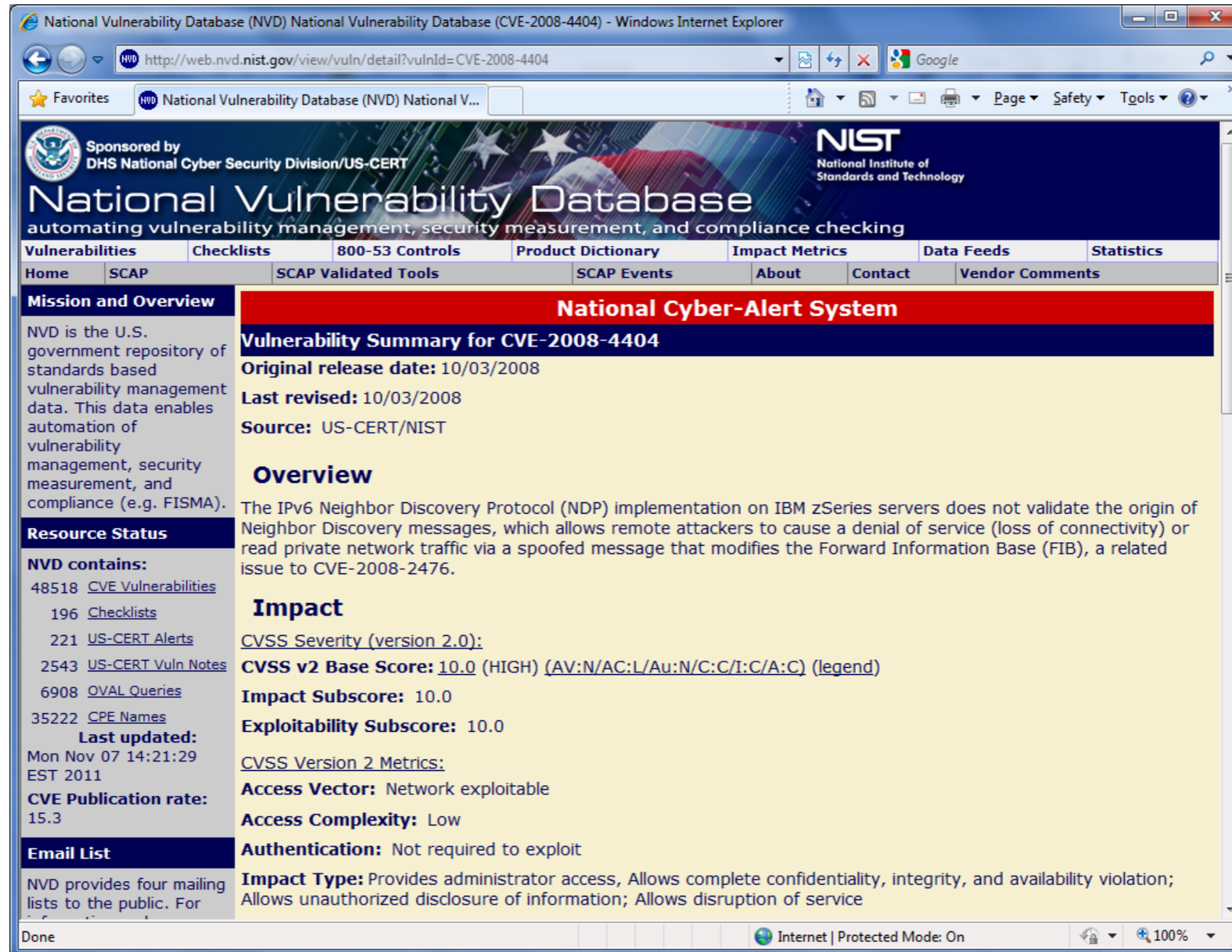
Done

Internet | Protected Mode: On

100%

Zanimivi primeri

Hack the Mainframe!



The screenshot shows a web browser window displaying the National Vulnerability Database (NVD) entry for CVE-2008-4404. The page is titled "National Vulnerability Database" and is sponsored by the DHS National Cyber Security Division/US-CERT. The main content area is titled "National Cyber-Alert System" and provides a "Vulnerability Summary for CVE-2008-4404".

Vulnerability Summary for CVE-2008-4404
Original release date: 10/03/2008
Last revised: 10/03/2008
Source: US-CERT/NIST

Overview
 The IPv6 Neighbor Discovery Protocol (NDP) implementation on IBM zSeries servers does not validate the origin of Neighbor Discovery messages, which allows remote attackers to cause a denial of service (loss of connectivity) or read private network traffic via a spoofed message that modifies the Forward Information Base (FIB), a related issue to CVE-2008-2476.

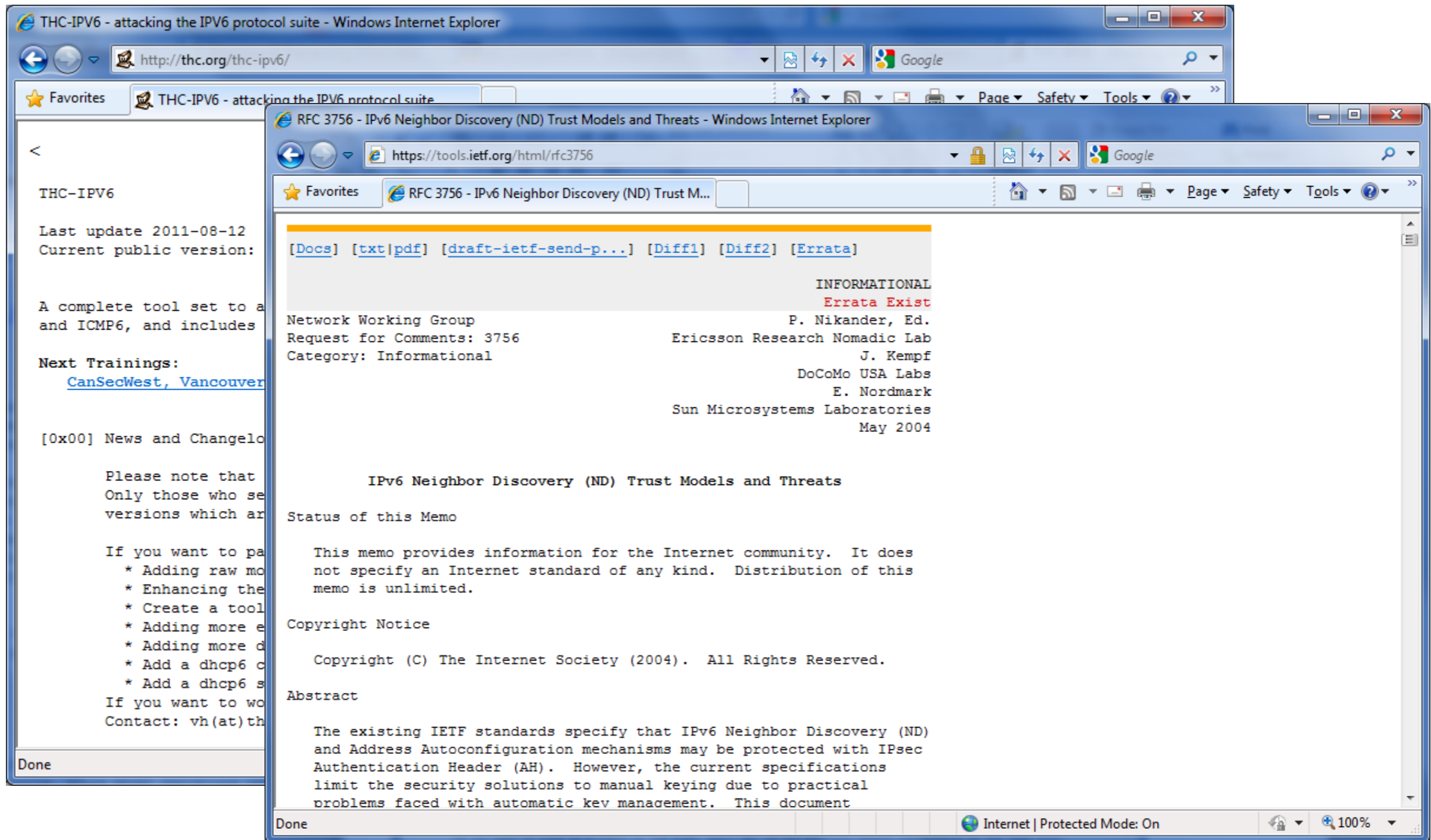
Impact
CVSS Severity (version 2.0):
CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:
Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

Resource Status
NVD contains:
 48518 [CVE Vulnerabilities](#)
 196 [Checklists](#)
 221 [US-CERT Alerts](#)
 2543 [US-CERT Vuln Notes](#)
 6908 [OVAL Queries](#)
 35222 [CPE Names](#)
Last updated: Mon Nov 07 14:21:29 EST 2011
CVE Publication rate: 15.3

Email List
 NVD provides four mailing lists to the public. For

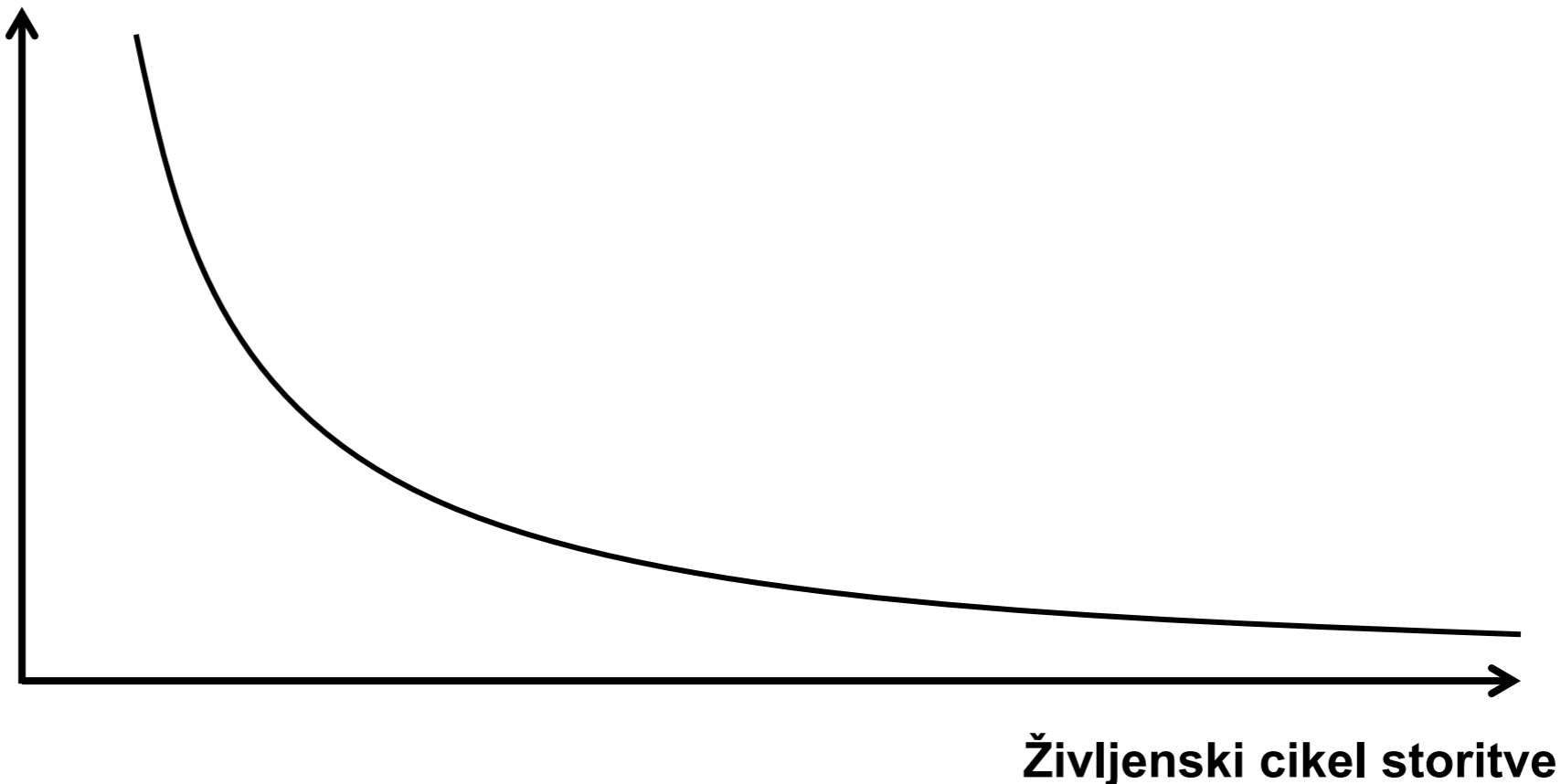
Panic!



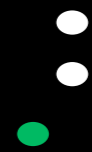
Back on track: Varni sistemi

- Varni sistemi so varno **načrtovani** in nato varno izvedeni in upravljeni
- Varnost mora biti zahtevana in upoštevana od dneva 0

Pripravljenost
izvedbe varnostnih
kontrol







Zelena polja

- Vpeljava IPv6 je ena EDINSTVENIH priložnosti v vaši karieri, da stvari naredite dobro na podlagi izkušenj z IPv4
- Kaj lahko izboljšate pri izvedbi IPv6?
 - Utrjenost infrastrukture in njenih procesov
 - Topologijo (npr. razslojenost omrežja)
 - Omrežne varnostne storitve
 - Minimizacijo dostopa
 - Preverjanje protokolov
 - Kriptografsko zaščito
- Ali imamo na voljo vso tehnologijo za to? (torej tisto, ki je najboljša praksa tudi na IPv4)



FLINTS

Remember IPv4?

- Kaj so bili najlažji problemi v IPv4
 - Varnost prenosa (VPN)
 - Utrjevanje infrastrukture
- Kaj so bili največji problemi omrežne varnosti na IPv4, ki so ostali nerešeni (oziroma, pogosto neizvedeni)
 - Varnost v LAN (prestrezanje, DoS)
 - Varnost usmerjanja (prestrezanje, DoS)
 - Verifikacija protokolov in aplikacijsko filtriranje v omrežju („whitelist“ model)
 - Tuneliranje

Infrastrukturno varovanje

Cisco IOS

IPv4

- CoPP (SW/HW)
- CPPr
- iACL
- RTBH
- Overjanje usmerjevalnih protokolov
- Overjanje izvora usmerjevalnih informacij

IPv6

- CoPP (SW/HW)
- iACL
- RTBH
- Overjanje usmerjevalnih protokolov
- Filtriranje usmerjevalnih informacij
- Overjanje izvora usmerjevalnih informacij

Varovanje med varnostnimi domenami

Cisco ASA: dinamični protokoli

Podprti dinamični protokoli nad IPv4

- FTP
- SIP
- DCERPC/MSRPC
- CTIQBE
- GTP
- H.323
- ILS
- MGCP
- MMP
- PPTP
- RSH
- RTSP
- SKINNY
- SQL*NET
- TFTP
- SUNRPC
- XDMCP

Podprti dinamični protokoli nad IPv6

- FTP
- SIP

Varovanje med varnostnimi domenami

Poljubna naprava: verifikacija in minimizacija protokolov/podatkov

Verifikacija protokolov

- Odmetavanje neskladnih protokolnih enot (L3-L7)
- Težave: neskladno obnašanje v legitimnih sejah
- Rešitev IPv4: ignoriranje vseh neskladnosti
- (alternativna rešitev: normalizacija protokolov)
- Posledica: izguba dragocene kontrole pred DoS/codeexec napadi

Minimizacija protokolov/podatkov

- Prepuščanje le najnujnejših protokolnih sporočil in podatkov (whitelisting)
- Težave: kdo ve, kaj je minimalno potreben nabor?
- Rešitev IPv4: prepuščamo ves promet v seji
- (alternativna rešitev: IPS)
- Posledica: izguba pasu (ali naramnic) in posledično hitrejša izguba hlač

Varovanje med varnostnimi domenami

Cisco IPS

Podpisi nad IPv4

Podpisi nad IPv6

5343

4999

Varovanje v LAN

Dostopnost ARP Inspection, DHCP Snooping, IP Source Guard

- Catalyst 2960
- Catalyst 3570
- Catalyst 3760
- Catalyst 4500
- Catalyst 6500
- Nexus 5000
- Nexus 7000
- ...

Dostopnost ND (SLAAC) Inspection

- Catalyst 6500

Implementacijske težave

- V varnostnih mehanizmih so in bodo še nekaj časa
- Še vedno imate bistveno bolj omejen problem, kot pri IPv4, in torej luksuz, da lažje testirate
- Aktivno rešujte težave na svoji poti – konfiguracijske in v kodi (preko proizvajalca ali FOSS skupnosti); ne čakajte na druge, saj so cikli popravkov pogosto dolgi
- Cilj naj bo, da stvari vedno delajo, ne da samo delajo

Povzetek

- IPv6 ne prinaša bistveno novih tveganj, morate pa ustrezno obravnavati vsa „nova stara“ tveganja
- Najboljša varnost na svetu je ta, ki je popolnoma prilagojena svojemu okolju
- Zdaj je pravi trenutek, ki ga ne boste več imeli
- Zelo dobro analizirajte svoje tehnološke možnosti za prenos kontrol v svet IPv6
- V IPv6 svetu boste (upam!) stvari večinoma naredili bolje kot v IPv4 – znanje prenesite nazaj v IPv4!
- Give back to the community! Skupaj izboljšajmo kakovost kontrol v IPv6!

Carpe IPv6 diem!

Ali pa vsaj pustite, da se od vas učimo...



MISTAKES

IT COULD BE THAT THE PURPOSE OF YOUR LIFE IS
ONLY TO SERVE AS A WARNING TO OTHERS.



Projekte zaključimo. Odnosi trajajo.