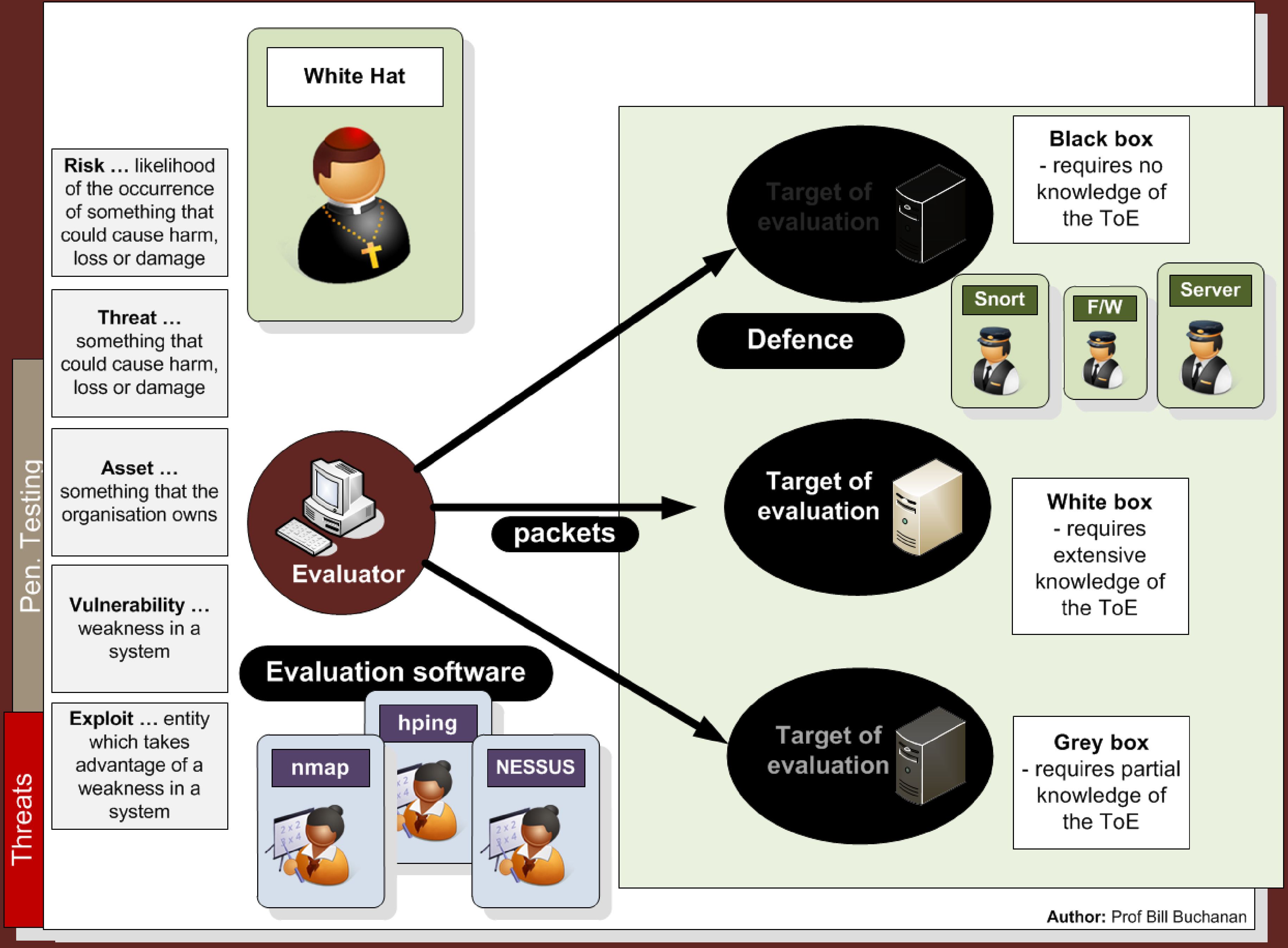
Digital

Investigator

Network Intrusions

Pen Testing: NESSUS



Risk … likelihood of the occurrence of something that could cause harm, loss or damage

Threat … something that could cause harm, loss or damage

Asset … something that the organisation owns

Vulnerability … weakness in a system

Exploit … entity which takes advantage of a weakness in a system

Black box - requires no knowledge of the ToE

White box - requires extensive knowledge of the ToE

Grey box - requires partial knowledge of the ToE

Author: Prof Bill Buchanan

White, grey and black box testing

Security Taxonomy

Introduction

A Threat:

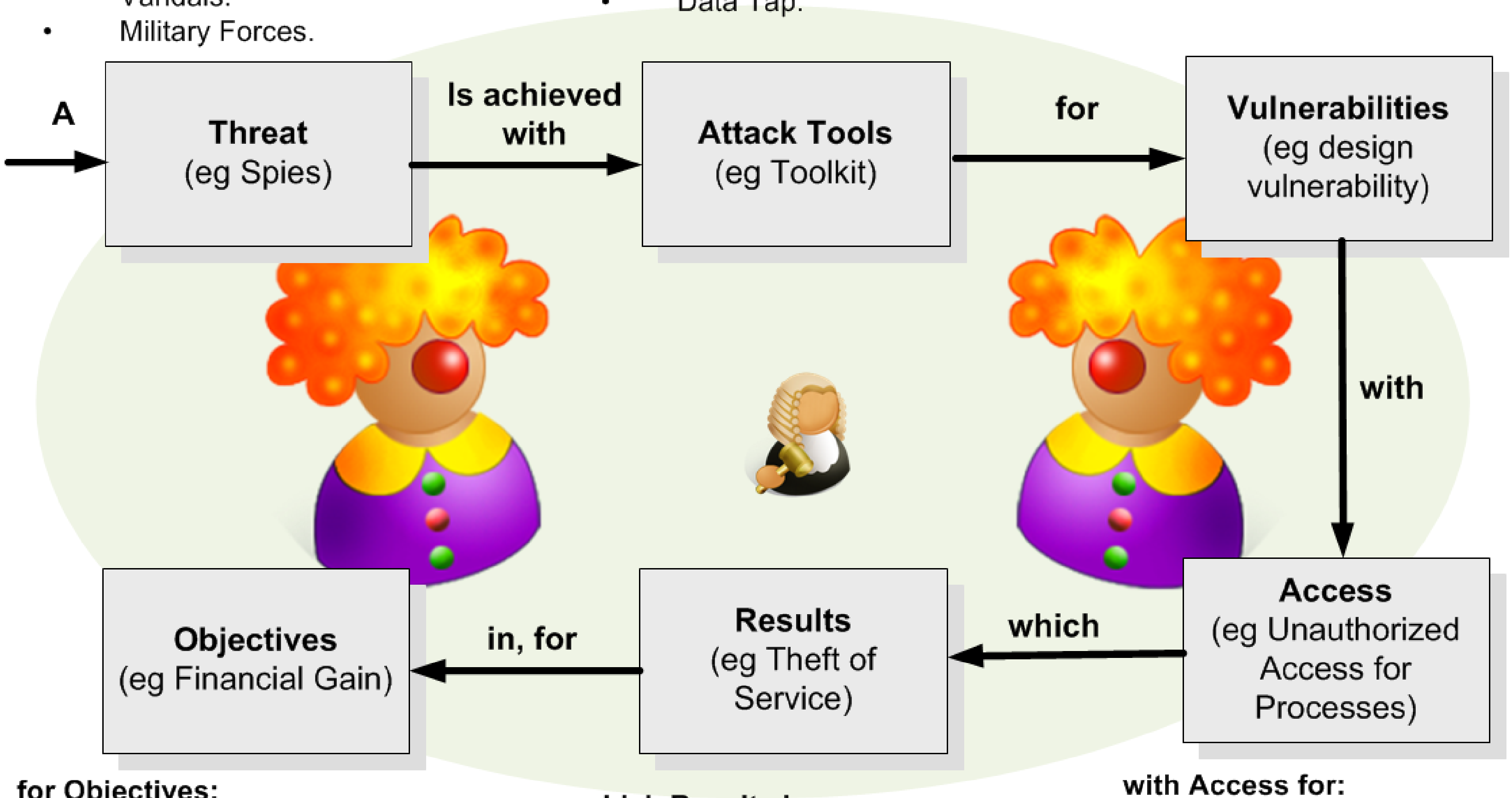
- Hacker.
- Spies
- Terrorists.
- Corporate Raiders.
- Professional Criminals.
- Vandals.
- Military Forces.

is achieved with Attack Tools:

- User command.
- Script or program.
- Autonomous Agent.
- Toolkit
- Distributed Tool.
- Data Tap.

for Vulnerabilities:

- Implementation vulnerability.
- Design vulnerability.
- Configuration vulnerability.



A

Threat
(eg Spies)

Is achieved with

Attack Tools
(eg Toolkit)

for

Vulnerabilities
(eg design vulnerability)

with

Access
(eg Unauthorized Access for Processes)

which

Results
(eg Theft of Service)

in, for

Objectives
(eg Financial Gain)

for Objectives:

- Challenge/Status.
- Political Gain.
- Financial Gain.
- Damage.
- Destruction of an Enemy.

which Results in:

- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:

- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan

Security Incident taxonomy

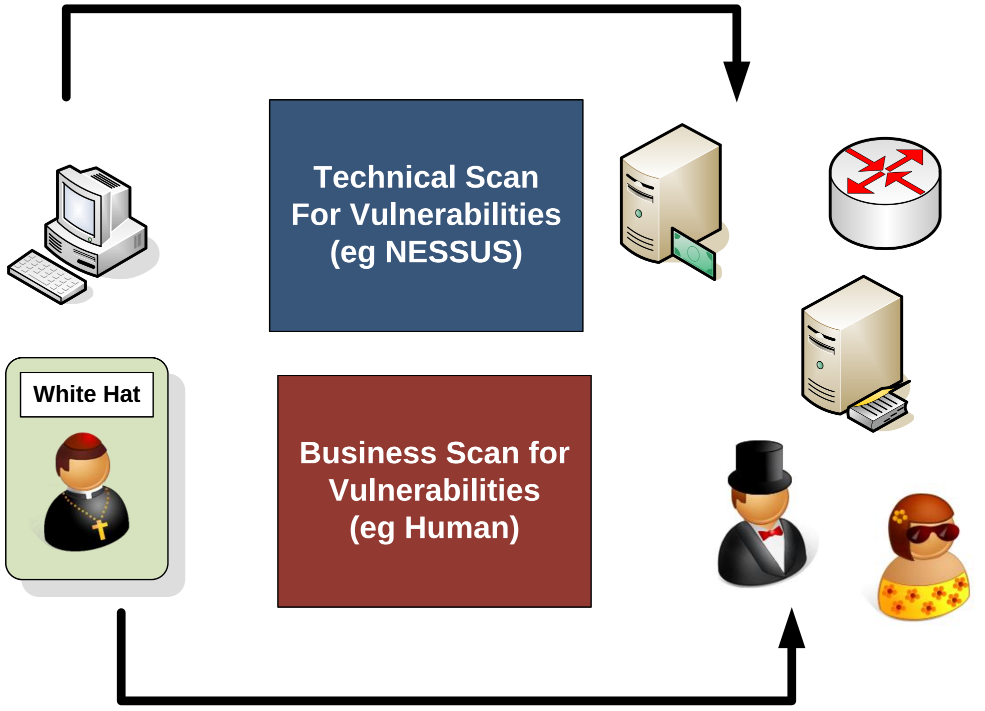
Pen Testing

Vulnerability

Threats

Automated Testing

- Port scanning.
- Malware detection.
- SQL Database Exploits.


Technical Scan For Vulnerabilities (eg NESSUS)
White Hat
Business Scan for Vulnerabilities (eg Human)

Adversarial Role

- Social Engineering.
- Password Cracking.
- Data Theft.

Risks

Adverse Disclosure
Service Availability
Business Disruption
Damage to or Modification to Assets
Fraud/E-Crime
Reputational Damage
Legal and Regulatory Censure

Threats

Malware
Hacking
Social
Misuse
Physical
Error
Environmental

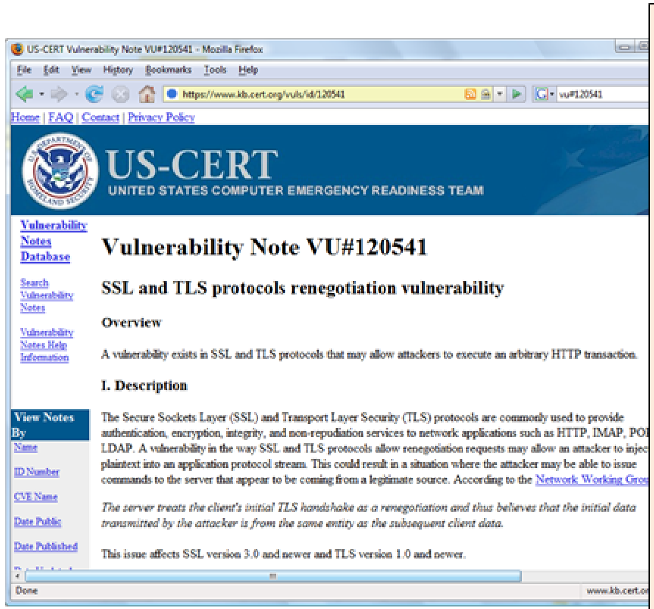
Actor

Internal
External
Trusted Partner

Author: Prof Bill Buchanan

Vulnerability

Threats


US-CERT Vulnerability Note VU#120541 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.kb.cert.org/vuls/id/120541
vu#120541
Home | FAQ | Contact | Privacy Policy
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
Vulnerability Notes Database
Search Vulnerability Notes
Vulnerability Notes Help Information
View Notes By
Name
ID Number
CVE Name
Date Public
Date Published
Done
www.kb.cert.o

Vulnerability Note VU#120541

SSL and TLS protocols renegotiation vulnerability

Overview

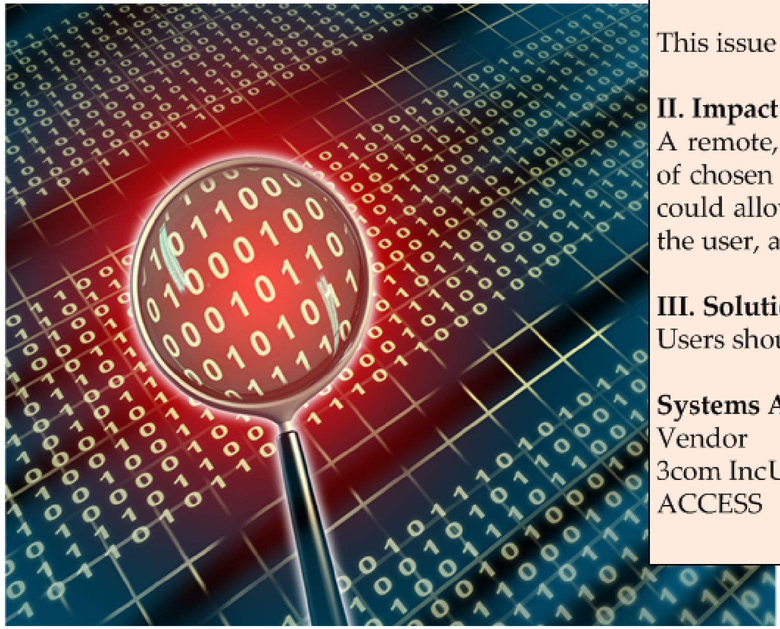
A vulnerability exists in SSL and TLS protocols that may allow attackers to execute an arbitrary HTTP transaction.

I. Description

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are commonly used to provide authentication, encryption, integrity, and non-repudiation services to network applications such as HTTP, IMAP, PO LDAP. A vulnerability in the way SSL and TLS protocols allow renegotiation requests may allow an attacker to injec plaintext into an application protocol stream. This could result in a situation where the attacker may be able to issue commands to the server that appear to be coming from a legitimate source. According to the Network Working Gro

The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data.

This issue affects SSL version 3.0 and newer and TLS version 1.0 and newer.



VU#120541: SSL and TLS protocols renegotiation vulnerability

Overview

A vulnerability exists in SSL and TLS protocols that may allow attackers to execute an arbitrary HTTP transaction.

I. Description

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are commonly used to provide authentication, encryption, integrity, and non-repudiation services to network applications such as HTTP, IMAP, POP3, LDAP. A vulnerability in the way SSL and TLS protocols allow renegotiation requests may allow an attacker to inject plaintext into an application protocol stream. This could result in a situation where the attacker may be able to issue commands to the server that appear to be coming from a legitimate source. According to the Network Working Group:

The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data.

This issue affects SSL version 3.0 and newer and TLS version 1.0 and newer.

II. Impact

A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.

III. Solution

Users should contact vendors for specific patch information.

Systems Affected

Vendor	Status	Date Notified	Date Updated
3com Inc	Unknown	2009-11-05	2009-11-05
ACCESS	Unknown	2009-11-05	2009-11-05

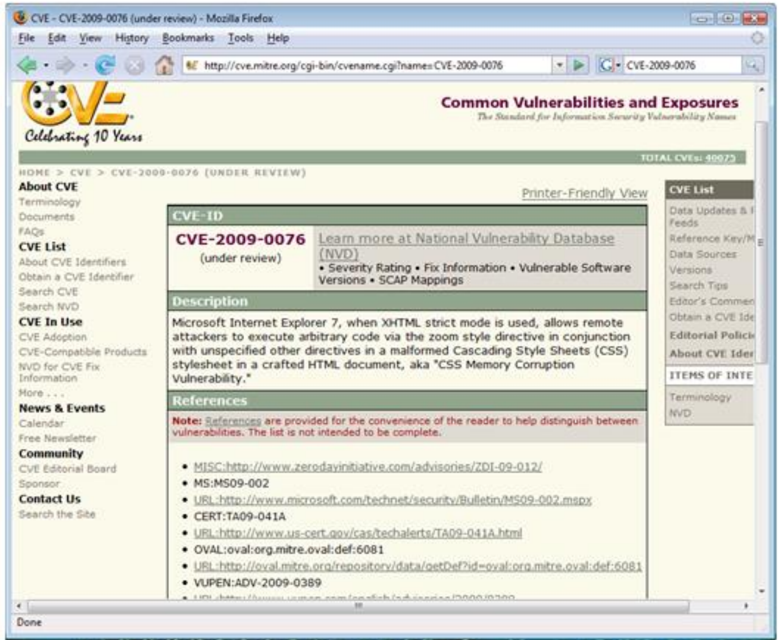
Author: Prof Bill Buchanan

US-CERT

NESSUS Database (CVE-ID)

Vulnerability

Threats



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

TOTAL CVEs: 40073

HOME > CVE > CVE-2009-0076 (UNDER REVIEW)

Printer-Friendly View

CVE-ID

CVE-2009-0076 (under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

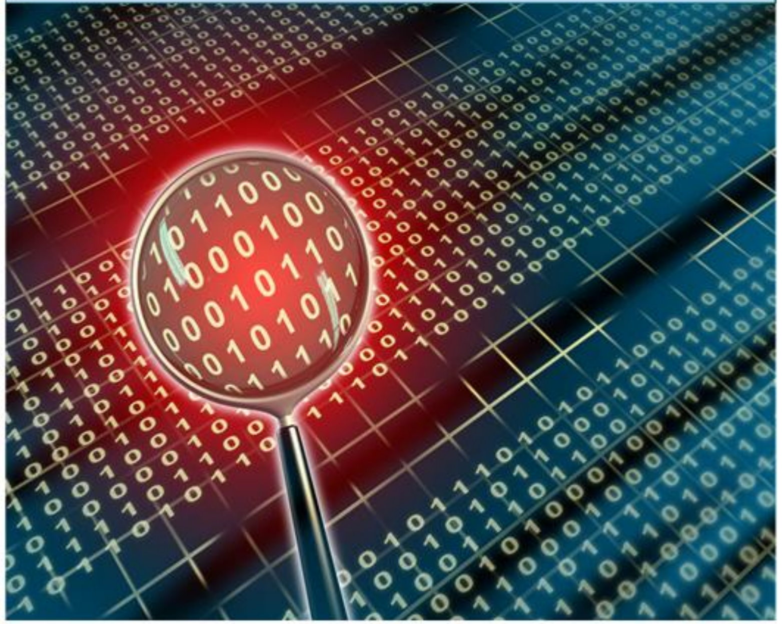
Description

Microsoft Internet Explorer 7, when XHTML strict mode is used, allows remote attackers to execute arbitrary code via the zoom style directive in conjunction with unspecified other directives in a malformed Cascading Style Sheets (CSS) stylesheet in a crafted HTML document, aka "CSS Memory Corruption Vulnerability."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://www.zerodayinitiative.com/advisories/ZDI-09-012/
- MS:MS09-002
- URL:http://www.microsoft.com/technet/security/Bulletin/MS09-002.mspx
- CERT:TA09-041A
- URL:http://www.us-cert.gov/cas/techalerts/TA09-041A.html
- OVAL:oval:org.mitre.oval:def:6081
- URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6081
- VUPEN:ADV-2009-0389



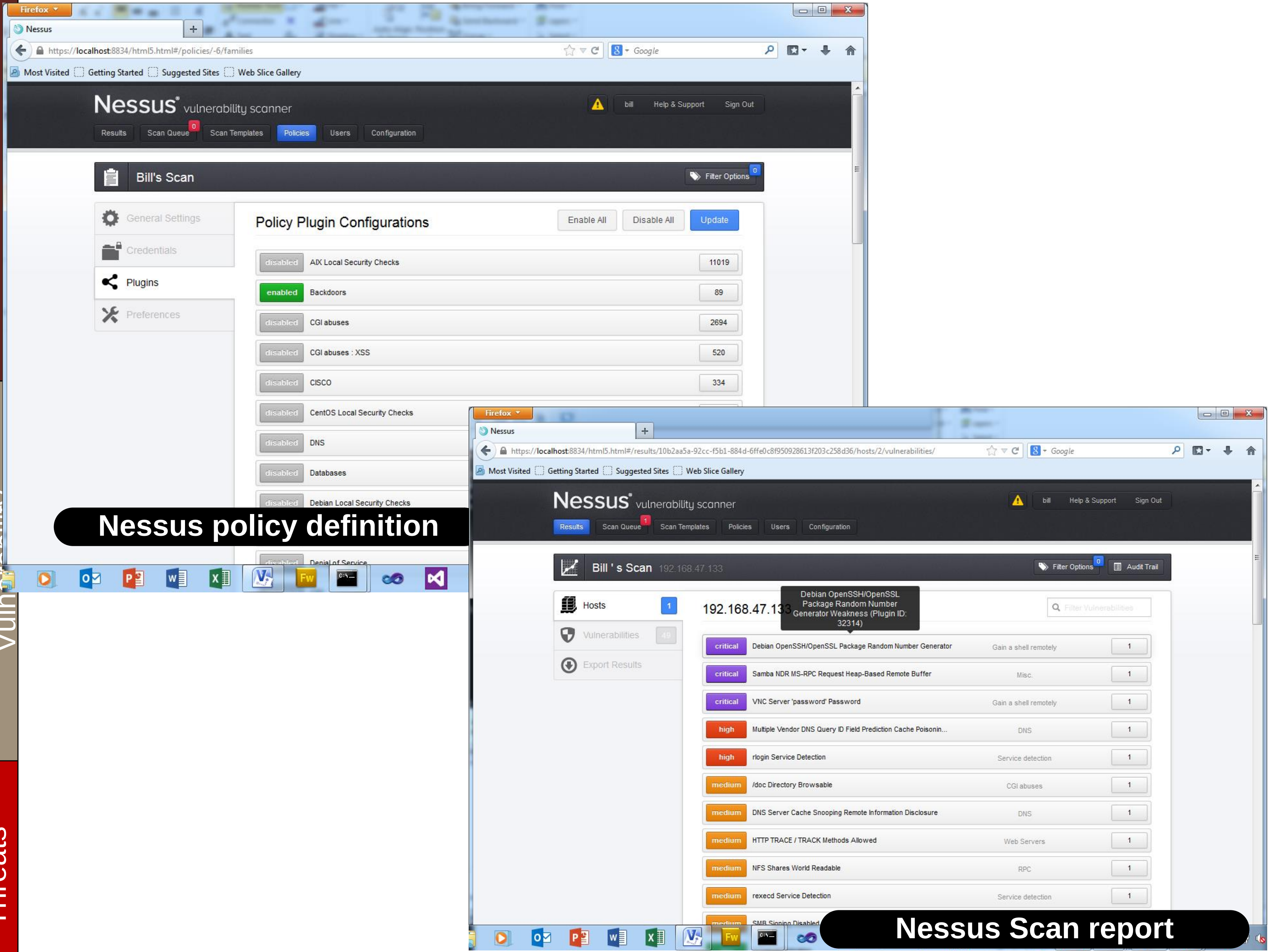
CVE-2009-0076

Summary: Microsoft Internet Explorer 7, when XHTML strict mode is used, allows remote attackers to execute arbitrary code via the zoom style directive in conjunction with unspecified other directives in a malformed Cascading Style Sheets (CSS) stylesheet in a crafted HTML document, aka "CSS Memory Corruption Vulnerability."

Published: 02/10/2009

CVSS Severity: 9.3 (HIGH)

Author: Prof Bill Buchanan



Policy Plugin Configurations

disabled	AIX Local Security Checks	11019
enabled	Backdoors	89
disabled	CGI abuses	2694
disabled	CGI abuses : XSS	520
disabled	CISCO	334
disabled	CentOS Local Security Checks	
disabled	DNS	
disabled	Databases	
disabled	Debian Local Security Checks	
disabled	Denial of Service	

Nessus policy definition

192.168.47.133

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (Plugin ID: 32314)

critical	Debian OpenSSH/OpenSSL Package Random Number Generator	Gain a shell remotely	1
critical	Samba NDR MS-RPC Request Heap-Based Remote Buffer	Misc.	1
critical	VNC Server 'password' Password	Gain a shell remotely	1
high	Multiple Vendor DNS Query ID Field Prediction Cache Poisonin...	DNS	1
high	rlogin Service Detection	Service detection	1
medium	/doc Directory Browsable	CGI abuses	1
medium	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
medium	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
medium	NFS Shares World Readable	RPC	1
medium	rexecd Service Detection	Service detection	1
medium	SMB Signing Disabled		

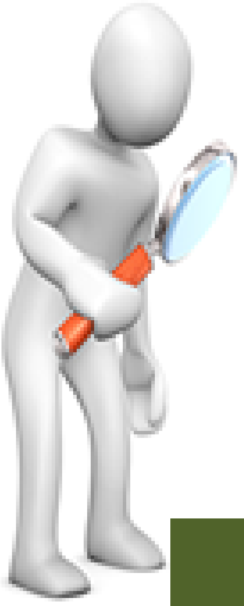
Nessus Scan report

Vulnerability

Threats

Author: Prof Bill Buchanan

NESSUS Scanner



Digital

Investigator

Network Intrusions

Pen Testing: NESSUS