Cyber-Infrastructure Uses for the NIST NSRL

Douglas White

NIST United States Department of Commerce
National Institute of Standards and Technology

Disclaimer

Trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

Statement of Disclosure

This research was funded by the National Institute of Standards and Technology Office of Law Enforcement Standards, the Department of Justice National Institute of Justice, the Federal Bureau of Investigation and the National Archives and Records Administration.

Overview

NSRL background

Common Platform Enumeration

Vulnerability identification

Related files

Location in RAM

Registry effects

Applicability

National Software Reference Librar

The NSRL collects software from various sources and incorporates file profiles computed from this software into a Reference Data Set (RDS) of information.

The RDS is used by law enforcement, government, and industry organizations to automatically identify files on a computer by matching file profiles in the RDS.

The RDS is a collection of digital signatures of known, traceable software applications.

National Software Reference Library

May, 2009

- over 10,000 software products of various types:
  - benign, malicious, corporate, electronic voting
- over 75,000,000 files

“Not a lending library”

- Building an environment in which researchers may access the files.

Common Platform Enumeration

CPE is a structured naming scheme for IT systems, platforms, and packages. CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name

NSRL is adopting the CPE scheme, to enable interoperability and automation of application searches

Previous methods of searching the NSRL for application required either free text searching or cryptographic hash matching.

cpe.mitre.org

Vulnerability Identification

The National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerabilit management data represented using the Security Content Automation Protocol (SCAP).

The NVD data enables automation of vulnerability management, security measurement, and compliance

When a vulnerability appears in the NVD, the CPE name is available as metadata.

nvd.nist.gov

Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute o
Standards and Tec
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Related Files

Given the CPE of a vulnerability, the metadata pertaining to a file or an environment can be found within the NSRL.

The cryptographic hashes can be used to evaluate the presence of critical files.

Other relationships within the application or operating system may be identified.

Location in RAM

NSRL has collaborated with investigators to hash normalized data sections of Windows® executable files and dynamically linked library (DLL) files.

Using the data hashes from EXE and DLL files, a RAM image can be parsed to identify applications which were resident.

This also can be mapped from a CVE, to determine the presence of a vulnerability.

Registry Effects

NSRL has a prototype Windows ® Registry Dataset (WiReD) available which enumerates a keys and values for applications in the Library.

Application installation, execution and deletion result in changes to the registry, and these hav been recorded.

www.nsrl.nist.gov/Downloads.htm

Applicability

NVD : Vulnerability Summary for CVE-2008-4817

Original release date:11/05/2008

Source: US-CERT/NIST

The Download Manager in Adobe Acrobat Professional and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a crafted PDF document that calls an AcroJS function with a long string argument, triggering heap corruption.

Vulnerable software and versions

* cpe:/a:adobe:acrobat:8.1.1 and previous versions

* cpe:/a:adobe:reader:8.1.2 and previous versions

Applicability

Using a Windows XP Pro system, Adobe Acrobat 8.0 was installed and used to view files. **cpe:/a:adobe:acrobat:8.0**

The NSRL has hashes and path locations for files in Acrobat 8.0; asset management information can be verified if needed.

The RAM hashes for executables in cpe:/a:adobe:acrobat:8.0 are available; forensics determined that executables and DLLs were loaded.

Registry settings were recorded.

HKEY_USERS\S-1-5-21-2000478354-117609710-839522115-500

\Software\Microsoft\Windows\ShellNoRoam\MUICache

C:\\Program Files\\Adobe\\Reader 8.0\\Reader\\AcroRd32.exe

Applicability

Adobe Acrobat 9.0 was installed (without removing 8.0) and used to view files. **cpe:/a:adobe:acrobat:9.0**

Again, the NSRL hashes and path locations were used t verify existence of files from Acrobat 8.0 and 9.0.

The RAM hashes for executables in cpe:/a:adobe:acrobat:9.0 are available; forensics determined that the 9.0 executable and DLLs were loaded.

Registry settings were recorded, and also showed 9.0 was accessed, not 8.0.

HKEY_USERS\S-1-5-21-2000478354-117609710-839522115-500

\Software\Microsoft\Windows\ShellNoRoam\MUICache

C:\\Program Files\\Adobe\\Reader 9.0\\Reader\\AcroRd32.exe

Contacts

Douglas White
www.nsrl.nist.gov
nsrl@nist.gov

Barbara Guttman
Software and Systems Division
barbara.guttman@nist.gov

Sue Ballou, Office of Law Enforcement Standards
Rep. For State/Local Law Enforcement
susan.ballou@nist.gov