[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

www.securityresearch.at

Semantic Potential of existing Security Advisory Standards

Secure Business Austria

Challenges

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Well maintained and audited IT infrastructure is critical for ensuring business continuity
  - Ever-growing complexity of IT environments
  - Legal regulations and rating systems (e.g., Basel II)
  - Numerous security alerts
    - majority is not structured for automatic processing

→ Management of networks and IT infrastructure elements is time-consuming and expensive

Challenges

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- CERT Coordination Center
  - Cataloged vulnerabilities doubled in the past three years (3780 in 2004; 7236 in 2007).
- Channels
  - 93% of the CSIRT constituents receive their incident information via email, 79% also via phone
  - RSS Feeds, Websites, faxes, SMS, …
  - →Unstructured and therefore not machine-processable


Microsoft Security Bulletin MS08-035 — Impo
Vulnerability in Active Directory Could Allow Denial of Ser
Published: June 10, 2008 | Updated: June 11, 2008
Version: 1.1
General Information
Executive Summary
This security update resolves a privately reported vulnerability in impl
Server 2008; Active Directory Application Mode (ADAM) when installed
(AD LDS) when installed on Windows Server 2008. The vulnerability c
Windows Server 2003, and Windows Server 2008, an attacker must h
vulnerability could cause the system to stop responding or automatica
This security update is rated Important for all supported editions of Mi
Server 2003, and Windows Server 2008. For more information, see th
The security update addresses the vulnerability by validating client LD
subsection for the specific vulnerability entry under the next section, V
Recommendation. Microsoft recommends that customers apply the
Known Issues. None
Top of section
Affected and Non-Affected Software
The following software have been tested to determine which versions
To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.
Affected Software
Products Affected
QuickTime, Security
QuickTime 7.5
QuickTime
CVE-ID: CVE-2008-1581
Available for: Windows Vista, XP SP2
Impact: Opening a maliciously crafted PICT image file may lead to an unexpected application termination or arbitrary code execution
Description: An issue in QuickTime's handling of PixData structures when processing a PICT image may result in a heap buffer overflow. Opening a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue through improved bounds checking. This issue does not affect systems running Mac OS X. Credit to Dyon Balding of Secunia Research for reporting this issue.
QuickTime
CVE-ID: CVE-2008-1582
Available for: Mac OS X v10.3.9, Mac OS X v10.4.9 - v10.4.11, Mac OS X v10.5 or later, Windows Vista, XP SP2
Impact: Opening a maliciously crafted AAC-encoded media content may lead to an unexpected application termination o
arbitrary code execution
Description: A memory corruption issue exists in QuickTime's handling of AAC-encoded media content. Opening a maliciously crafted media file may lead to an unexpected application termination or arbitrary code execution. This updat
addresses the issue by performing additional validation of media files. Credit to Dave Soldera of NGS Software, and Jens Alfke for reporting this issue.

Software	Component	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by This Update
Microsoft Windows 2000 Server Service Pack 4	Active Directory (KB949014)	Denial of Service	Important	MS08-003
Windows XP Professional Service Pack 2	ADAM	Denial of Service	Moderate	MS08-003

CSIRT

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- CSIRT (Computer Security Incident Response Team)
  - Reactive Services (Incident Handling, Alerts and Warnings, …)
  - Proactive Services (Configuration, Technology Watch, Announcements,…)
  - Security Quality Management Services (Risk Analysis, Training, …)
- Advisory Messages
  - Describe computer security problems and/or solutions

Contribution

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Introduction of a collection of existing security advisory standards
- Review and evaluation of those standards

Evaluation

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Goal
  - Identification of semantic usable standards
- Criteria
  - Semantic Usability
    - Does the standard use a standardized language such as XML to ensure machine-readability?
    - Does the standard provide clear and unambiguous semantics to ensure machine-recognition?
  - Information Complexity
    - Does the standard provide the necessary elements for describing IT incidents? A comprehensive and well defined set of elements is required to describe IT incidents in the most granular form.
    - Does the standard offer the possibility for a complete workaround for an IT incident or does it simply provide links to external resources?

Evaluation

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Distribution
  - Is this standard used by any major CSIRTs?
  - Is it still supported? When was the last update?
  - The usage and support by major CSIRTs is crucial for the acceptance of the semantic security advisory standard within the community.

ANML

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Advisory and Notification Markup Language
- XML-based specification for advisories and other types of notifications
- Open Security Project (OpenSec)
- Aims to solve inconsistent use of terminology
  - Benefit for the community and vendors
- Notifications: bug-fixes, feature enhancements, upgrade availability,…
- Description, Status, Affected, Assessments, Update, Verify, and Revision History

ANML Example

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

```
<?xml version="1.0" encoding="utf-8" ?>
   …
   <subject>Unchecked Buffer In Windows…</subject>
   <dateCreated>2003-03-17</dateCreated>

   <status>
         <vendor>Confirmed</vendor>
         <severity>Critical</severity>
         <class>Buffer overflow</class>
         …
   </status>
   <summary>...</summary>
   <affected>
         <system id="WinNT“>
               <os>
                     <name>Windows NT 4.0</name>
                     <productType>Server</productType>
                     <productType>Workstation</productType>
               </os>
         </system>

   …
```

ANML

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Semantic usability ~
  - Introduction of "RDF" element
  - Allows the usage of free text fields
    - OS name, productType, .. "xs:string" ("Windows" / "Win")
    - SDML, SIML
- Information complexity ~
  - Missing information (e.g., vendor, software on operating systems, and CVE ref.)
- Distribution –
  - No major CSIRTs are currently using ANML, last update 2003

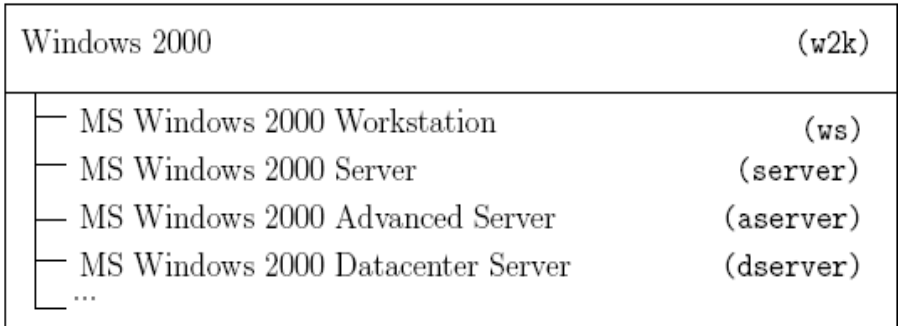
EISPP

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- European Information Security Promotion Programme
  - Advisory Format - precise and timely information about new vulnerabilities
- EU-funded (5th framework programme)
- June 2002 until January 2004
- Cert-IST, esCERT-UPC, SIEMENS-CERT, Callineb Consulting, I-NET, CLUSIT and InetSecur
- Basic: Complete Identification (CVE, Bugtrag ID,…), Vulnerability Classification, System Information, Problem Description and Solution

EISPP

- Semantic usability ~
  - Due to this flexibility, cooperating organizations sometimes need a further explanation of their usage conventions (free text fields)
  - e.g., <FormattedText>Foo v1.3 on BAR OS</FormattedText>
  - Common Model of System Information (CMSI)
- Information complexity ~
  - Missing attributes such as required reboot, software and hardware vendor



- Distribution +
  - German CERT-Verbund uses the EISPP extension DAF

CAIF

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Common Announcement Interchange Format
- Exchange and store security advisories
  - multi-lingual textual descriptions
  - different renderings (Markup)
- RUS-CERT
- Identification (target-group)
- Affected System (OVAL linking possible)
- identification, target-groups?, revisions, category, subject, summary, affected?, workaround?, solution?, …

CAIF

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Semantic usability ~
- MTEXT, UTEXT (e.g., affected systems)

```
<!ENTITY % MTEXT       "(
            %UTEXT; | p | b | vb | em |  pre | vendor | program | file | aff | update | …)“
```

- Information complexity ~
  - e.g., affected system and its operating system, patch level, and vendor are not described by distinct elements
- Distribution ~
  - Some middle-sized and company-owned CSIRTs use the CAIF advisory standard

IODEF

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Incident Object Description Exchange Format
- Common data format for describing and exchanging incident information between CSIRTs
- IETF Extended Incident Handling (INCH) Working Group
- IDMEF compatibility
- Covers the entire attack (including e.g., log files)

IODEF

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Semantic usability ~
  - Overlapping elements such as Incident and EventData
- Information complexity -
  - No information on affected files, patch location (URL), or potential workaround
- Distribution +
  - Some vulnerability management tools are able to handle IODEF messages; Oct-10-2007: accepted for RFC publication

OVAL

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Open Vulnerability and Assessment Language
- US-CERT / U.S. Department of Homeland Security
- Transfer & expression of public available security content
- Assessment Process
  - System Characteristics
  - Analysis (vulnerability, configuration, patch state, …)
  - Results schema

OVAL

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Semantic usability +
  - Well-defined and semantically usable
- Information complexity ~
  - Highly granular but missing patch information and predefined product lists (CPE in new versions “<reference source="CPE“ ref_id="cpe:/o:microsoft:windows_2003::gold:itanium"/>”)
- Distribution +
  - OVAL is supported and used by several governmental and commercial organizations, Various existing tools

Conclusion

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

- Evaluation of existing security advisory standards
- OVAL standard is the most suitable standard for the automatic or semi-automatic interpretation of security advisories

→ Faster reaction times and avoidance of interpretation errors for newly-discovered vulnerabilities

Contact

[SECURE]
Business Austria
Kompetenz für Wissenschaft und Industrie.

Andreas Ekelhart

aekelhart@securityresearch.at