



# Cisco Security IntelliShield Alert Manager Service



## Technical Overview

# Cisco Security IntelliShield Alert Manager Service

## What

Provides timely, detailed intelligence and alerting on threats and vulnerabilities

## For

Organizations that need proactive, early warning on emerging threats, vulnerabilities, and safeguards

## Value

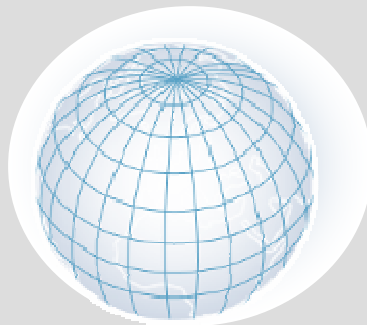
- Proactive discovery and notification of vulnerabilities
- Intelligence on the impacted applications and associated patches
- Faster remediation of potential vulnerabilities
- Avoid potential security outbreaks and associated costs

The screenshot displays the Cisco Security IntelliShield Alert Manager interface. The top navigation bar includes 'Home | Support | Library | Help | Logout' and the 'IntelliShield' logo. The main content area is titled 'Alerts' and features an 'Advanced Search' section with a search box and a 'Search' button. Below the search section is a table of alerts with the following columns: IntelliShield ID, Headline, Published EST, Version, Urgency, Credibility, Severity, CVSS Base, CVSS Temporal, and Notify. The table lists various vulnerabilities, such as 'Apple QuickTime UDTA Atom Integer Overflow Vulnerability' (ID 12798) and 'Mozilla Firefox SVG Mosaic Buffer Overflow Vulnerability' (ID 12743). The bottom of the interface shows 'Total Alerts = 11767' and 'Total Pages = 589'.

IntelliShield ID	Headline	Published EST	Version	Urgency	Credibility	Severity	CVSS Base	CVSS Temporal	Notify
12798	Apple QuickTime UDTA Atom Integer Overflow Vulnerability	Mar 06 2007 10:49 AM	1	High	High	Critical	8.0	5.3	Notify
12743	Mozilla Firefox SVG Mosaic Buffer Overflow Vulnerability	Mar 06 2007 10:49 AM	2	High	High	Critical	8.0	5.3	Notify
12799	Apple QuickTime PICT File Buffer Overflow Vulnerability	Mar 06 2007 10:45 AM	1	High	High	Critical	8.0	5.3	Notify
12753	Mozilla Firefox and SeaMonkey Blocked Pop-up Window Cross-SL	Mar 06 2007 10:28 AM	2	High	High	Critical	1.9	1.4	Notify
12749	Mozilla Firefox and SeaMonkey Nonalpha-non-dgit Filter Eva	Mar 06 2007 10:19 AM	2	High	High	Critical	8.0	5.9	Notify
12740	Mozilla Network Security Services: SSLv2 Client Integer Under	Mar 06 2007 10:14 AM	3	High	High	Critical	8.0	5.9	Notify
12742	Mozilla Firefox, SeaMonkey, and Thunderbird Layout Engine Me	Mar 06 2007 9:58 AM	2	High	High	Critical	8.0	5.9	Notify
12794	IntelliShield Daily Virus Report For March 6, 2007	Mar 06 2007 9:58 AM	1	High	High	Critical			Notify
12750	Mozilla Firefox and SeaMonkey Blocked Range Local File Access	Mar 06 2007 9:56 AM	2	High	High	Critical	1.9	1.4	Notify
12797	Apple QuickTime Movie File Buffer Overflow Vulnerability	Mar 06 2007 9:43 AM	1	High	High	Critical	8.0	5.3	Notify
12760	Mozilla Firefox and SeaMonkey onUnload Event Handler Memory	Mar 06 2007 9:20 AM	2	High	High	Critical	8.0	5.3	Notify
12796	Apple QuickTime MIDI File Buffer Overflow Vulnerability	Mar 06 2007 9:02 AM	1	High	High	Critical	8.0	5.3	Notify
12795	Apple QuickTime 3GP File Integer Overflow Vulnerability	Mar 06 2007 8:57 AM	1	High	High	Critical	8.0	5.3	Notify
12762	Trojan.Trojan.Pirfame	Mar 06 2007 8:08 AM	2	High	High	Critical			Notify
12695	PostgreSQL Query Planner Data Type Check Bypass Issue	Mar 06 2007 5:20 AM	7	High	High	Critical			Notify
12693	PostgreSQL Data Type Change Denial of Service Issue	Mar 06 2007 5:14 AM	10	High	High	Critical			Notify
12784	IntelliShield Periodic Security Activity Report: February 26	Mar 05 2007 6:28 PM	1	High	High	Critical			Notify
12793	IntelliShield Activity Report: Apple QuickTime Multiple Code	Mar 05 2007 5:47 PM	1	High	High	Critical			Notify
12792	IntelliShield Activity Report: Multiple PHP Vulnerabilities	Mar 05 2007 5:33 PM	1	High	High	Critical			Notify
11741	Linux/Unix: GNUzip Null Pointer Dereference Denial of Serv	Mar 05 2007 5:27 PM	12	High	High	Critical	2.3	1.6	Notify

# IntelliShield Service Overview

## Global Source Network



Security Organizations  
Product Vendors  
Government Sources  
Antivirus Vendors  
Mailing Lists  
Cisco Security Research

## Security Intelligence Operations



Collect and Evaluate  
Analyze and Correlate  
Disseminate

## Fused and Filtered Intelligence on Vulnerabilities, Malicious Codes, Security Trends

**Linux Kernel Bluetooth Support CAPI Packet Buffer Overflow Vulnerability**

Severity: <b>Critical</b>	Confidence: <b>Confirmed</b>
Priority: <b>High</b>	Security: <b>Medium to Severe</b>
CVSS Base: <b>9.0</b>	CVSS Temporal: <b>8.6</b>
CVSS Impact: <b>Low</b>	CVE Category: <b>CVE-2008-1338</b>

**Description:** The Linux kernel versions 2.22.4 and prior and 2.6.19.1 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code.

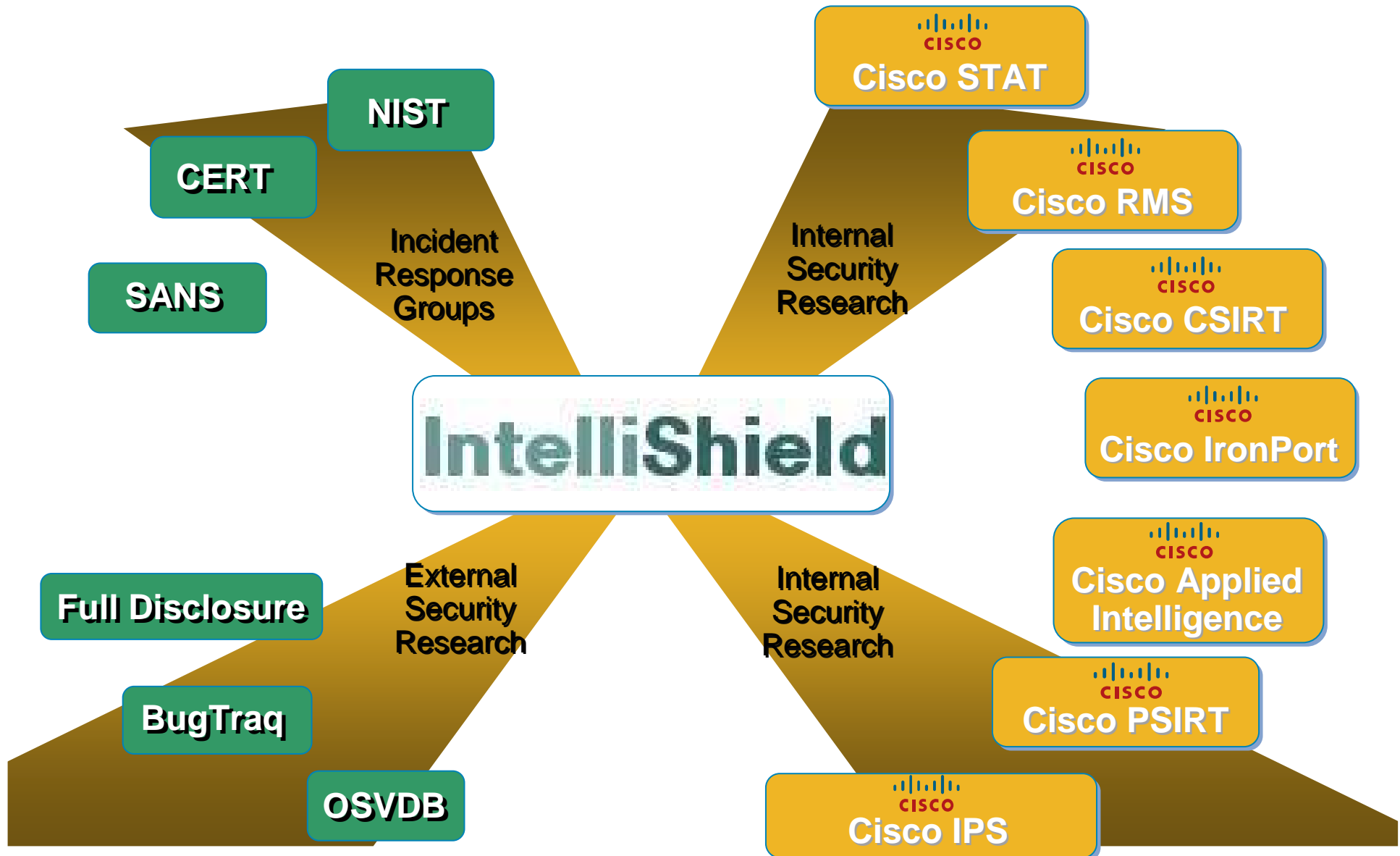
**Technical Information:** To exploit this vulnerability, an attacker must be able to supply a specially crafted CAPI packet to a vulnerable system. The attacker must also be able to establish a connection to an IEEE 802.15.1 compliant device that supports CAPI. The vulnerability could be used to execute arbitrary code on the target system.

**Working Solution:** The following versions of the Linux kernel are vulnerable:  
Linux kernel 2.22.4 and prior  
Linux kernel 2.6.19.1 and prior

## Customized Notification, Tasking, Auditing, Reporting



# Sources of Security Intelligence



# Features and Functions

**Alerts**

**Advanced Search**

Search:  For:

**CVSS Calculator**

IntelliShield ID	Headline	Published EST	Version	Urgency	Credibility	Severity	CVSS Base	CVSS Temporal	Notify
12798	Apple QuickTime UDTA Atoms Integer Overflow Vulnerability	Mar 06 2007 10:49 AM	1				8.0	5.9	Notify
12743	Mozilla Firefox SVG Viewer Buffer Overflow Vulnerability	Mar 06 2007 10:48 AM	2				8.0	6.3	Notify
12799	Apple QuickTime PICT File Buffer Overflow Vulnerability	Mar 06 2007 10:45 AM	1				8.0	5.9	Notify
12753	Mozilla Firefox and SeaMonkey Blocked Pop-up Window Cross-Si	Mar 06 2007 10:28 AM	2				1.9	1.4	Notify
12749	Mozilla Firefox and SeaMonkey Non-alpha-non-digit Filter Eva	Mar 06 2007 10:19 AM	2						Notify
12740	Mozilla Network Security Services SSLv2 Client Integer Under	Mar 06 2007 10:14 AM	3				8.0	5.9	Notify
12742	Mozilla Firefox, SeaMonkey, and Thunderbird Layout Engine Me	Mar 06 2007 9:58 AM	2				8.0	5.9	Notify
12794	IntelliShield Daily Virus Report For March 6, 2007	Mar 06 2007 9:58 AM	1						Notify
12750	Mozilla Firefox and SeaMonkey Blocked Popup Local File Acces	Mar 06 2007 9:56 AM	2				1.9	1.4	Notify
12797	Apple QuickTime Movie File Buffer Overflow Vulnerability	Mar 06 2007 9:43 AM	1				8.0	5.9	Notify
12760	Mozilla Firefox and SeaMonkey onUnload Event Handler Memory	Mar 06 2007 9:20 AM	2				8.0	6.3	Notify
12796	Apple QuickTime MIDI File Buffer Overflow Vulnerability	Mar 06 2007 9:02 AM	1				8.0	5.9	Notify
12795	Apple QuickTime 3GP File Integer Overflow Vulnerability	Mar 06 2007 8:57 AM	1				8.0	5.9	Notify
12762	Trojan: Trojan.Pirlames	Mar 06 2007 8:08 AM	2						Notify
12605	PostgreSQL Query Planner Data Type Check Bypass Issue	Mar 06 2007 5:20 AM	7						Notify
12603	PostgreSQL Data Type Change Denial of Service Issue	Mar 06 2007 5:14 AM	10						Notify
12784	IntelliShield Periodic Security Activity Report: February 26	Mar 05 2007 6:28 PM	1						Notify
12793	IntelliShield Activity Report: Apple QuickTime Multiple Code	Mar 05 2007 5:47 PM	1						Notify
12792	IntelliShield Activity Report: Multiple PHP Vulnerabilities	Mar 05 2007 5:33 PM	1						Notify
11741	Linux/Unix: GNU gzip Null Pointer Dereference Denial of Serv	Mar 05 2007 5:27 PM	12				2.3	1.6	Notify

Total Alerts = 11767 Total Pages = 589

- Comprehensive threat and vulnerability database
- User-defined technology profiles
- Customized notifications
- Tasking and workflow management
- Cisco IPS Signature correlation
- Optional XML Feed

# IntelliShield Database

**Advanced Search**

[Basic Search](#) [Search Tips](#)

**Vendor:**

**Product:**

**Version:**

**Product Type:**

**Client:**

**Group:**

**Product Set:**

**Keyword:**

**IntelliShield ID:**

**Urgency:**

**Credibility:**

**Severity:**

**CVSS Base:**

**CVSS Temporal:**

**Published Before EST:**

**Published After EST:**

**Alert Type:**

- Access to over 14,000 Alerts dating back to May of 2000
- Advanced search feature allows clients to perform in-depth research and analysis

# User-Defined Technology Profiles

**Edit Profile Details** | **Add Product To Profiles** | **View Profile Report**

Client Name: Demo    Group Name: Security    Product Set Name: Windows

Product Type: Application    Vendor name:     Contains    Product name:     Contains  
 Starts With     Starts With

**Vendor**  
Mewsoft  
Michael Baumer  
Michael Hipp  
Michael Jennings  
Michael Lamont  
Michael Roth Software  
Michael Trojnara  
Microburst Technologies, Inc.  
Micromuse, Inc.  
Microsoft, Inc. **INCLUDE**

**Product**  
Windows NT Workstation 4.0 Option Pack  
Windows Scripting Host  
Windows Server 2003  
Windows Server 2003, Datacenter Edition  
Windows Server 2003, Enterprise Edition  
Windows Server 2003, Standard Edition  
Windows Server 2003, Web Edition  
Windows Services for UNIX  
Windows SharePoint Services  
Windows XP **EXCLUDE**

**Version Release**  
Original Release  
Home Edition  
Professional Edition  
Professional Edition, 64-bit (Itanium)  
Professional x64 (AMD/EM64T)  
Tablet PC Edition  
Media Center Edition  
**INCLUDE**    **EXCLUDE**

**ServicePack/Platform**  
Base  
SP1  
SP2 **INCLUDE**    **EXCLUDE**

Copyright 2006 Cisco Systems, Inc.

- Create product sets based on technologies relevant to your infrastructure
- The ability to customize at different levels—vendor, product, version, or service pack

# Customized Notifications

**Edit Notification**

Urgency: 3  
Credibility: 2  
Severity: 4

\*Alert Type(s):  
Daily Virus Report  
Flash Alert  
Geopolitical Analysis Report  
Intelligence Bulletin  
Malicious Code Alert  
Security Issue Report  
Vulnerability Alert

**Step 3: Select Alert Products which will Generate this Notification**

Include All Products

Or, Please select from the following:

Available Product Sets:  
IBM AIX  
Linux  
Malicious Code  
Openwall Linux  
Red Hat Linux  
Unix

Selected Product Sets:  
Windows

Add >  
< Remove  
Clear

Users	Group	Role	Task	Pager/SMS	Email	Message
<a href="#">Beckwith, Matt</a>	Security	Viewer	<input type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<a href="#">Smith, Joe</a>	Security	Group Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Notifications are defined by technology profiles as well as the rating (Urgency, Credibility, and Severity)
- Customers are only notified of vulnerabilities and threats that are relevant to their pre-defined infrastructure

# Tasking and Workflow Management

>> [Alert Manager](#) >> [Inbox](#) >> [Details](#)

**View Inbox Item**

**Client:** Demo **Group:** Help Desk  
**Description:** Linux Kernel search\_binary\_handler Denial of Service Vulnerability **Priority:** 1  
**Due Date:** Feb 10, 2006 **Last Update Date:** Feb 02, 2006  
**Alert:** 9937 **Date Completed:**

**Audit Trail:**

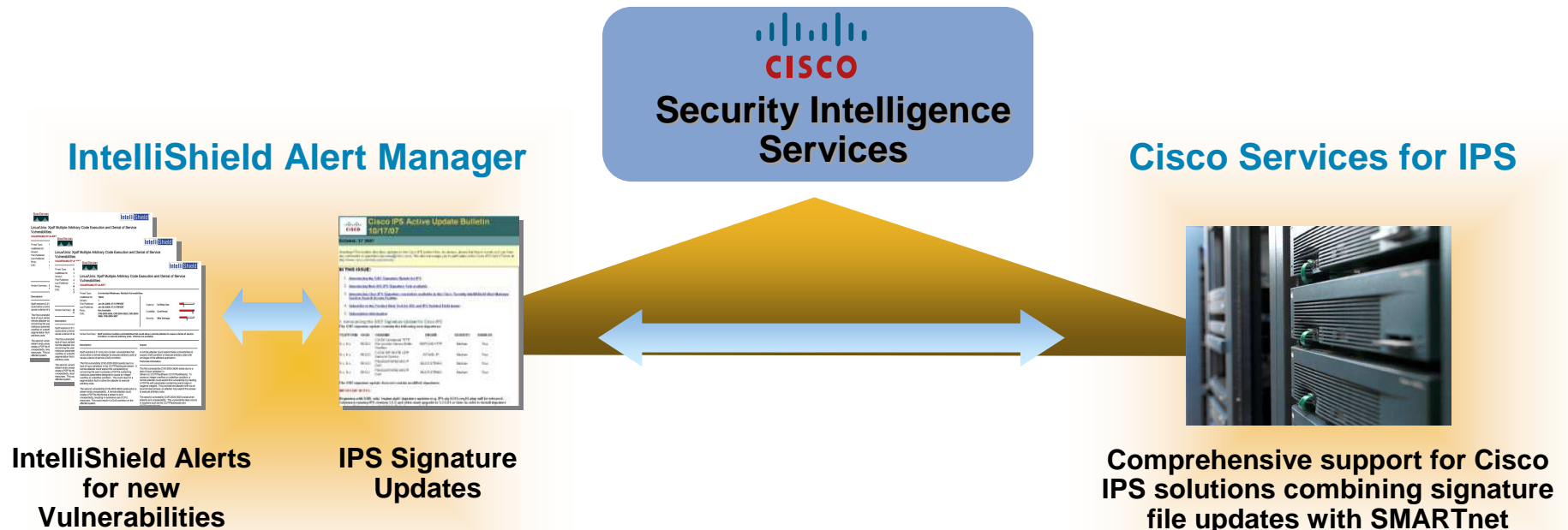
2006-02-02 11:05:37.29
Matt Beckwith
Thank you.
2006-02-02 11:04:55.52
Joe Smith
We are currently reviewing the updated packages and will notify you once we deployed them.
2006-02-02 11:03:33.07
Matt Beckwith
Please apply the updates by COB next Friday.

**Assigned To:**

Users	Group	Role	Task	Pager/SMS	Email	Message
Smith, Joe	Help Desk	Group Admin	Yes	No	No	No

- Assign tasks to individuals and share critical information across the enterprise
- View what tasks are outstanding, who is assigned each task, as well as the current status of remediation efforts

# Cisco IPS Signature Correlation With IntelliShield Alerts



## IPS Signature Correlation with IntelliShield Alerts

- Access the latest vulnerabilities and threats with correlated Cisco IPS Signature information: signature name, signature ID, release version, and release date

## Cisco Services for IPS customers receive:

- Full access to the IntelliShield Search Access feature to search for alerts related to IPS signatures
- Ability to search comprehensive database of Cisco IPS Signature information



# IntelliShield Alert Manager XML Service

- Simple and secure solution to retrieve all IntelliShield threat and vulnerability data
- Integrate content into existing applications



# IntelliShield Alerts




- Vulnerability Alert
- Malicious Code Alert
- Daily Malicious Code Summary
- Security Activity Bulletin
- Security Issue Alert
- Geopolitical Security Alert
- Cyber Risk Report
- Applied Mitigation Bulletin
- Flash Alert



### Linux Kernel Bluetooth Support CAPI Packet Buffer Overflow Vulnerability

**VULNERABILITY ALERT**

---

Threat Type:	<b>Unintended Weakness: Buffer Overflow</b>	Urgency:	<b>Weakness Found</b>	
IntelliShield ID:	<b>12294</b>	Credibility:	<b>Confirmed</b>	
Version:	<b>15</b>	Severity:	<b>Moderate Damage</b>	
First Published:	<b>Dec 18, 2006; 11:56 AM EST</b>	CVSS Base:	<b>10.0</b>	<a href="#">CVSS Calculator</a>
Last Published:	<b>Jun 18, 2007; 08:24 AM EDT</b>	CVSS Temporal:	<b>7.4</b>	CVSS Version 1.0
Vector:	<b>Remote</b>			
Authentication:	<b>Not Required</b>			
Exploit:	<b>No</b>			
Port:	<b>Not Available</b>			
CVE:	<b>CVE-2006-6106</b>			
BugTraq ID:	<b>21604</b>			

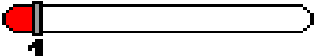
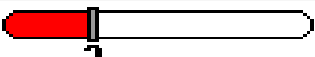
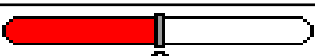
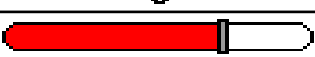

---

Version Summary: **Debian has released a security advisory and updated packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.**

---

Description	Impact
The Linux Kernel versions 2.4.33.4 and prior and 2.6.19.1 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code.	An unauthenticated, remote attacker could exploit this vulnerability to cause a DoS condition or execute arbitrary code with root privileges. As a result, the attacker could take complete control of the affected system.
The vulnerability exists because the kernel's Bluetooth stack fails to sufficiently validate input. An unauthenticated, remote attacker could exploit this vulnerability by submitting malicious CMTMP messages to an affected host. This action could cause a buffer overflow condition and allow the attacker to cause a DoS condition or execute arbitrary code with root privileges.	<b>Technical Information</b> To exploit this vulnerability, an attacker must be able to submit a malicious CMTMP message to an affected host. The attacker must submit the message via a device connected to an ISDN network that the target system resides on. The vulnerability exists because the <code>cmtp_recv_interopmsg</code> function of the kernel's Bluetooth support ( <code>net/bluetooth/cmtp/capi.c</code> ) fails to properly perform input validation. An unauthenticated, remote attacker could exploit this vulnerability by submitting malicious CMTMP packets designed to exploit a boundary error in <code>cmtp_recv_interopmsg</code> . This action could cause the kernel to overwrite kernel CMTMP and CAPI data structures allowing the attacker to cause a DoS condition or execute arbitrary code with root privileges.
Kernel.org confirmed this vulnerability with a changelog and released updated software.	
<b>Warning Indicators</b> The following versions of the Linux Kernel are vulnerable:  Linux Kernel 2.4.33.4 and prior Linux Kernel 2.6.19.1 and prior	

# IntelliShield Risk Rating System

	Urgency	Credibility	Severity
	Weakness	Very Low	No Damage
	Unlikely Use	Low	Harassment
	Possible Use	Corroborated	Minor Damage
	Probable Use	Highly Credible	Moderate Damage
	Incidents Reported	Confirmed	Heavy Damage

- **Urgency:** The likelihood that a discovered weakness or attack method may be employed
- **Credibility:** Defines how real the reported threat is based upon sources that are used to gain the information and the technical correctness of that information
- **Severity:** Quantifies the possible effect of an attack in terms of its impact

# Sections of an Alert

**CISCO** **IntelliShield**

**Linux Kernel Bluetooth Support CAPI Packet Buffer Overflow Vulnerability**  
*VULNERABILITY ALERT*

Threat Type: **Unintended Weakness: Buffer Overflow**

IntelliShield ID: **12294**

Version: **15**

First Published: **Dec 18, 2006; 11:56 AM EST**

Last Published: **Jun 18, 2007; 08:24 AM EDT**

Vector: **Remote**

Authentication: **Not Required**

Exploit: **No**

Port: **Not Available**

CVE: **CVE-2006-6106**

BugTraq ID: **21604**

Urgency: **Weakness Found** (1)

Credibility: **Confirmed** (5)

Severity: **Moderate Damage** (4)

CVSS Base: **10.0** [CVSS Calculator](#)

CVSS Temporal: **7.4** (CVSS Version 1.0)

Version Summary: **Debian has released a security advisory and updated packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.**

**Description**

The Linux Kernel versions 2.4.33.4 and prior and 2.6.19.1 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code.

The vulnerability exists because the kernel's Bluetooth stack fails to sufficiently validate input. An unauthenticated, remote attacker could exploit this vulnerability by submitting malicious CMTMP messages to an affected host. This action could cause a buffer overflow condition and allow the attacker to cause a DoS condition or execute arbitrary code with root privileges.

Kernel.org confirmed this vulnerability with a changelog and released updated software.

**Impact**

An unauthenticated, remote attacker could exploit this vulnerability to cause a DoS condition or execute arbitrary code with root privileges. As a result, the attacker could take complete control of the affected system.

**Technical Information**

To exploit this vulnerability, an attacker must be able to submit a malicious CMTMP message to an affected host. The attacker must submit the message via a device connected to an ISDN network that the target system resides on. The vulnerability exists because the `cmtp_recv_interopmsg` function of the kernel's Bluetooth support (`net/bluetooth/cmtplcap.c`) fails to properly perform input validation. An unauthenticated, remote attacker could exploit this vulnerability by submitting malicious CMTMP packets designed to exploit a boundary error in `cmtp_recv_interopmsg`. This action could cause the kernel to overwrite kernel CMTMP and CAPI data structures allowing the attacker to cause a DoS condition or execute arbitrary code with root privileges.

**Warning Indicators**

The following versions of the Linux Kernel are vulnerable:

- Linux Kernel 2.4.33.4 and prior
- Linux Kernel 2.6.19.1 and prior

## Risk Ratings

Each Alert graded by urgency, credibility, severity, and CVSS industry standard

## Version Summary

Brief summary of the most recent Alert version

## Description

High level overview of Alert and strategic implications

## Impact

The possible effect of an attack

## Technical Information

Tactical explanations and guidance aimed at administrators

# Actionable Intelligence

**IntelliShield Analysis**  
 Security analysts provide additional analysis and comments regarding the alert

**Safeguards**  
 Workarounds and mitigation information

**Patches/Software**  
 Applicable patches and software available for download

**Vendor Announcements**  
 Links to associated vendor advisories

<p><b>IntelliShield Analysis</b></p> <p>To exploit this vulnerability, the attacker must deliver CMTF packets to the affected system. No further user interaction is required. Because Bluetooth-connected ISDN devices are not widely used, attackers are unlikely to exploit this vulnerability. Users of Bluetooth-connected ISDN TAs or routers are advised to upgrade to a non-affected kernel.</p> <p>The CAPI message transport protocol (CMTF) delivers Common ISDN application programming interface (CAPI) data.</p> <p>The 2.6 branch of kernels distributed by some third-party vendors may include the vulnerable functionality. Administrators are advised to contact their Linux vendor to determine whether they are affected.</p>	<p><b>Safeguards</b></p> <p>Administrators are advised to apply the appropriate update.</p> <p>Administrators are advised to disable Bluetooth support if not necessary for business operations.</p> <p>Administrators may consider issuing ISDN devices to users that do not connect via Bluetooth.</p>
<p><b>Vendor Announcements</b></p> <p>Summaries of changes are available at the following links: <a href="#">Linux Kernel 2.4.33.5 changelog</a> and <a href="#">Linux Kernel 2.6.19.2 changelog</a></p> <p>Avaya has released a security advisory at the following link: <a href="#">ASA-2007-063</a></p> <p>Debian has released a security advisory at the following link: <a href="#">DSA-1304-1</a></p> <p>Mandriva has released security advisories at the following links: <a href="#">MDKSA-2007-002</a>, <a href="#">MDKSA-2007-012</a>, and <a href="#">MDKSA-2007-025</a></p> <p>Red Hat has released a security advisory at the following link: <a href="#">RHSA-2007-0014-6</a></p> <p>SUSE has released security announcements at the following links: <a href="#">SUSE-SA-2007-018</a>, <a href="#">SUSE-SA-2007-021</a>, <a href="#">SUSE-SA-2007-030</a> and <a href="#">SUSE-SA-2007-035</a></p> <p>Trustix has released a security advisory at the following link: <a href="#">TSLSA-2007-0002</a></p> <p>Ubuntu Linux has released security notices at the following links: <a href="#">USN-416-1</a> and <a href="#">USN-416-2</a></p>	<p><b>Patches/Software</b></p> <p>Updated versions are available at the following links: <a href="#">Linux Kernel 2.4.33.5</a> and <a href="#">Linux Kernel 2.6.19.2</a></p> <p>Debian has released updated packages at the following link: <a href="#">Debian</a></p> <p>Mandriva can be updated automatically using <b>MandrivaUpdate</b>. Mandrake can be updated automatically using <b>MandrakeUpdate</b>.</p> <p>Red Hat packages can be updated using the <b>up2date</b> command.</p> <p>SUSE has released updated packages; users can install the updates using the YaST utility.</p> <p>Trustix has released updated packages at the following link:</p> <p>Trustix 2.2 - <a href="#">kernel-2.4.34-1tr</a></p> <p>Ubuntu Linux has released updated packages at the following links:</p> <p><b>Ubuntu 5.10</b>  <a href="#">linux-image-2.6.12-10-386 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-686 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-686-smp 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-amd64-generic 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-amd64-k8 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-amd64-k8-smp 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-amd64-xeon 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-k7 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-k7-smp 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-powerpc 2.6.12-10.45</a>  <a href="#">linux-image-2.6.12-10-powerpc-smp 2.6.12-10.45</a></p>

# “Filtered” Intelligence

**Alert History**  
Provides a timeline summarizing each time the Alert was updated with new information

**Product Sets**  
Smart-Filters to reduce “noise” and drive applicable Intelligence to appropriate audience

**Alert History**

**Version 8, February 12, 2007, 12:43 PM:** Ubuntu Linux has released a security notice and updated packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.

**Version 7, January 30, 2007, 4:59 PM:** Kernel.org has released a software changelog along with updated versions to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.

**Version 6, January 30, 2007, 2:39 PM:** Red Hat has released a security advisory and updated packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.

**Version 5, January 24, 2007, 8:42 AM:** Mandriva has released a security advisory and updated packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.

**Version 4, January 16, 2007, 1:05 PM:** Mandriva has released a security advisory and updated packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.

**Version 3, January 5, 2007, 9:48 AM:** Trustix has released a security advisory and updates packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.

**Version 2, January 3, 2007, 8:16 AM:** Mandriva has released a security advisory and updates packages to address the Bluetooth support CAPI packet buffer overflow vulnerability in the Linux Kernel.

**Version 1, December 18, 2006, 11:56 AM:** The Linux Kernel contains a buffer overflow vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service condition or execute arbitrary code. Updates are available.

---

**Product Sets**

The security vulnerability applies to the following combinations of products.

*Primary Products:*

		2.4.0   2.4.1   2.4.2   2.4.3   2.4.4   2.4.5   2.4.6   2.4.7   2.4.8   2.4.9   2.4.10   2.4.11   2.4.12   2.4.13   2.4.14   2.4.15   2.4.16   2.4.17   2.4.18   2.4.19   2.4.20   2.4.21   2.4.22   2.4.23   2.4.24   2.4.25   2.4.26   2.4.27   2.4.28   2.4.29   2.4.30   2.4.31   2.4.32   2.4.33 Base, .1, .2, .3, .4   2.6.0   2.6.1   2.6.2   2.6.3   2.6.4   2.6.5   2.6.6   2.6.7   2.6.8   2.6.9   2.6.10   2.6.11 Base, .1, .2, .3, .4, .5, .6, .7, .8, .9, .10, .11   2.6.12 Base, .1, .2, .3, .4, .5   2.6.13 Base, .1, .2, .3, .4   2.6.14 Base, .1, .2, .3, .4, .5, .6, .7   2.6.15 Base, .1, .2, .3, .4, .5, .6, .7   2.6.16 Base, .1, .2, .3, .4, .5, .6, .7, .8, .9, .10, .11, .12, .13, .14, .15, .16, .17, .18, .19, .20, .21, .22, .23, .24, .25, .26, .27, .28, .29, .30, .31   2.6.17 Base, .1, .2, .3, .4, .5, .6, .7, .8, .9, .10, .11, .12, .13, .14   2.6.18 .0, .1, .2, .3   2.6.19 Base, .1
<b>Linus Torvalds</b>	Linux Kernel	

*Associated Products:*

<b>Avaya, Inc.</b>	Application Enablement Services (AES)	4.0
<b>Avaya, Inc.</b>	Converged Communications Server (CCS)	2.0 Base, .1   2.1   3.0   3.1 Base, .1
<b>Avaya, Inc.</b>	Modular Messaging	3.0
<b>Avaya, Inc.</b>	S8300 Media Center	2.0 (Communication Manager)   2.0.1 (Communication Manager)   2.1 (Communication Manager)   2.1.1 (Communication Manager)   2.2 (Communication Manager)   3.0 (Communication Manager)   3.1 (Communication Manager)



