Cisco Security IntelliShield Alert Manager Service

Technical Overview

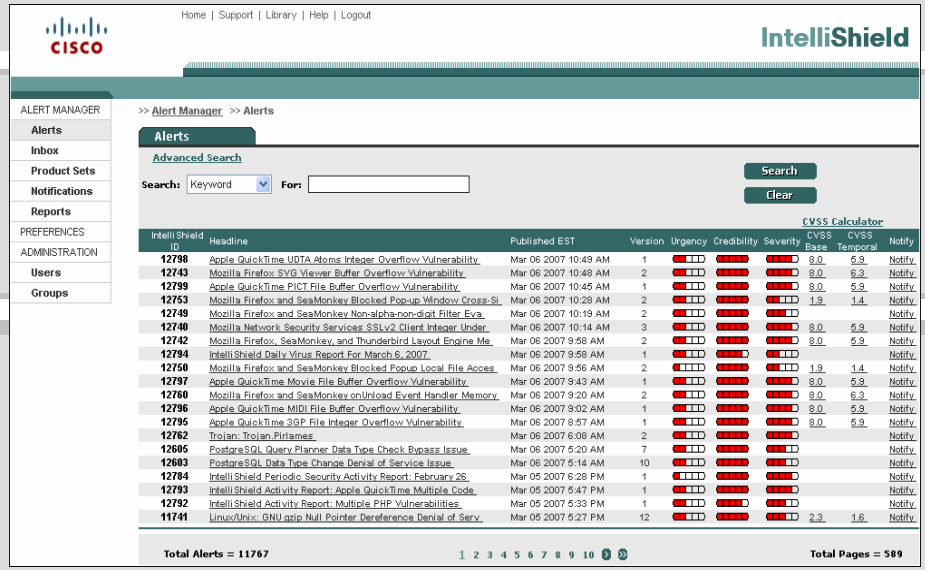
Cisco Security IntelliShield Alert Manager Service

What

Provides timely, detailed intelligence and alerting on threats and vulnerabilities

For

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

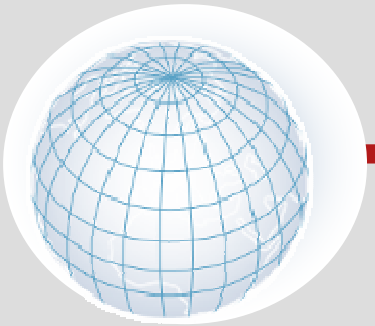


Value

- **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**

IntelliShield Service Overview

Global Source Network



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

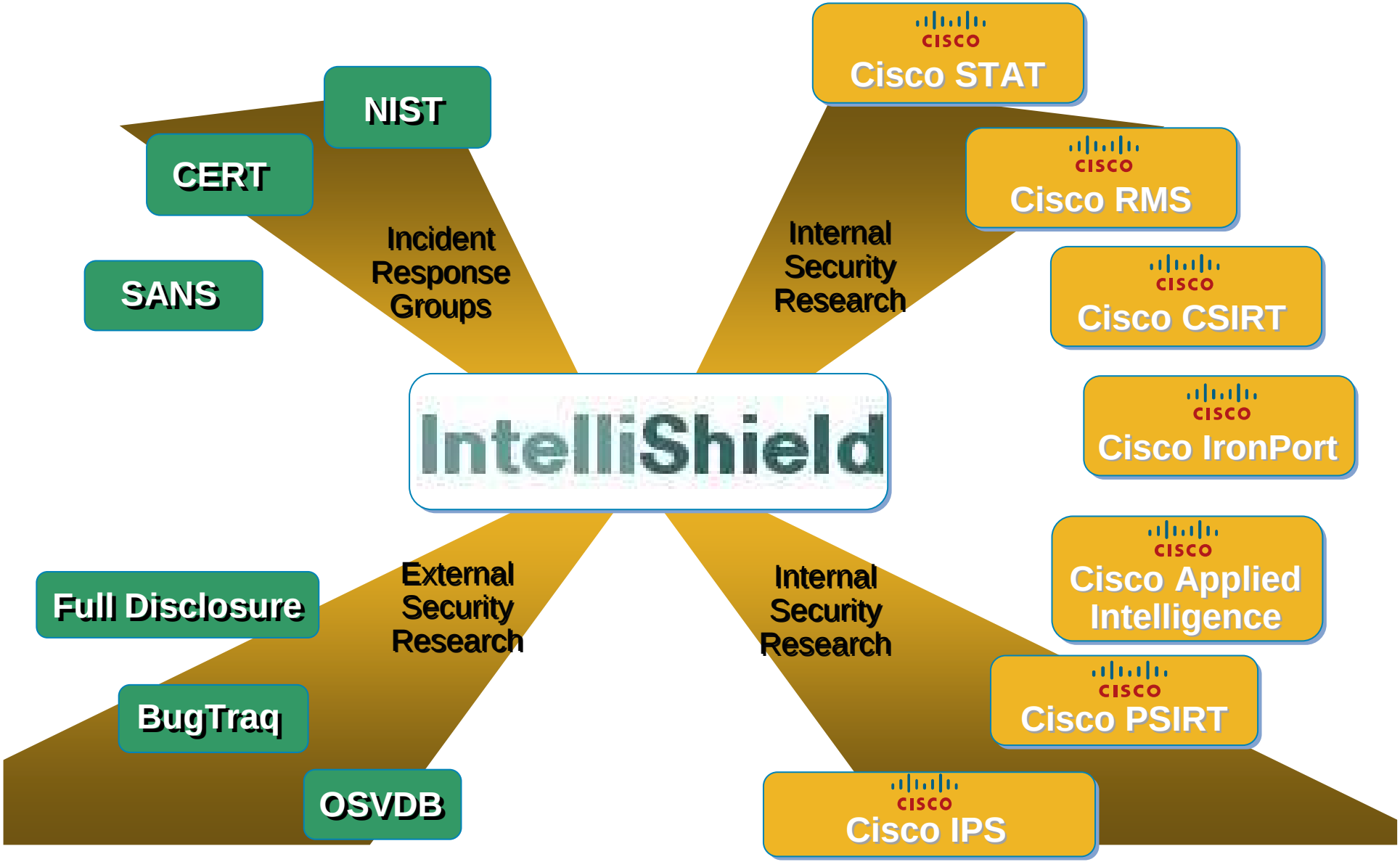
Security Intelligence Operations

Collect and Evaluate
Analyze and Correlate
Disseminate

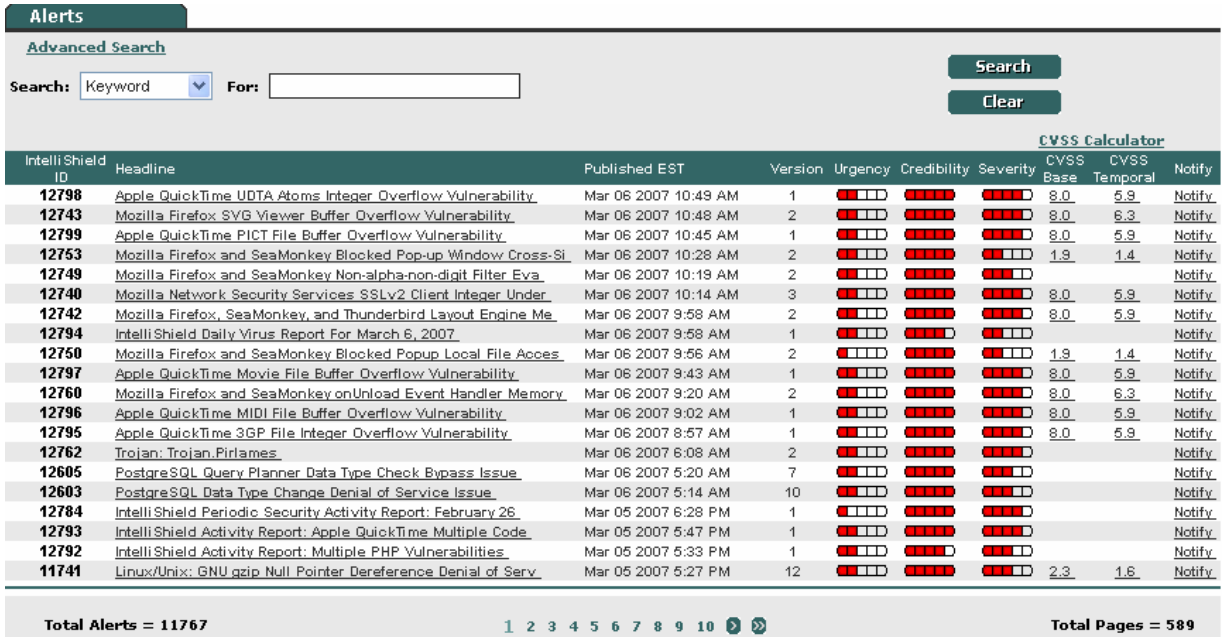
Fused and Filtered Intelligence on Vulnerabilities, Malicious Codes, Security Trends

Customized Notification, Tasking, Auditing, Reporting

Sources of Security Intelligence



Features and Functions



Alerts

Advanced Search

Search: Keyword For:

Search

Clear

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	6.9	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	6.9	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	6.9	Notify
12742	Mozilla Firefox, SeaMonkey, and Thunderbird Layout Engine Me	Mar 06 2007 9:58 AM	2				8.0	6.9	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	6.9	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	6.9	Notify
12795	Apple QuickTime 3GP File Integer Overflow Vulnerability	Mar 06 2007 8:57 AM	1				8.0	6.9	Notify
12762	Trojan: Trojan.Pirlames	Mar 06 2007 6:08 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

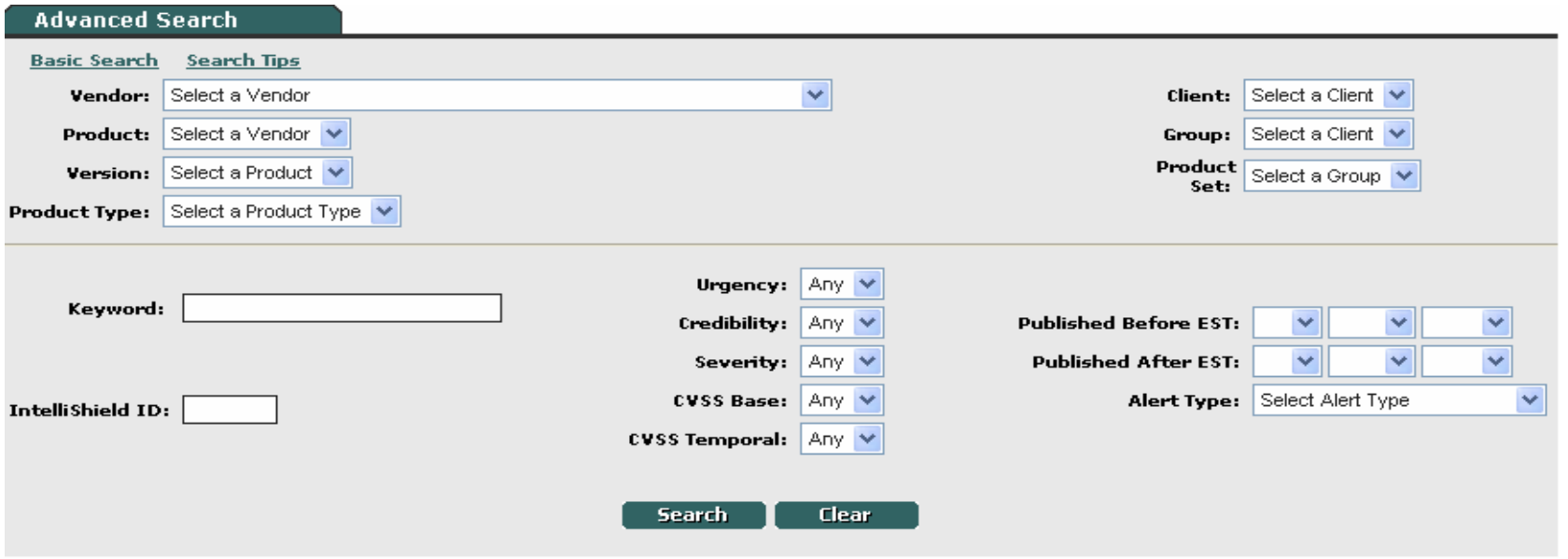
Total Alerts = 11767

1 2 3 4 5 6 7 8 9 10

Total Pages = 589

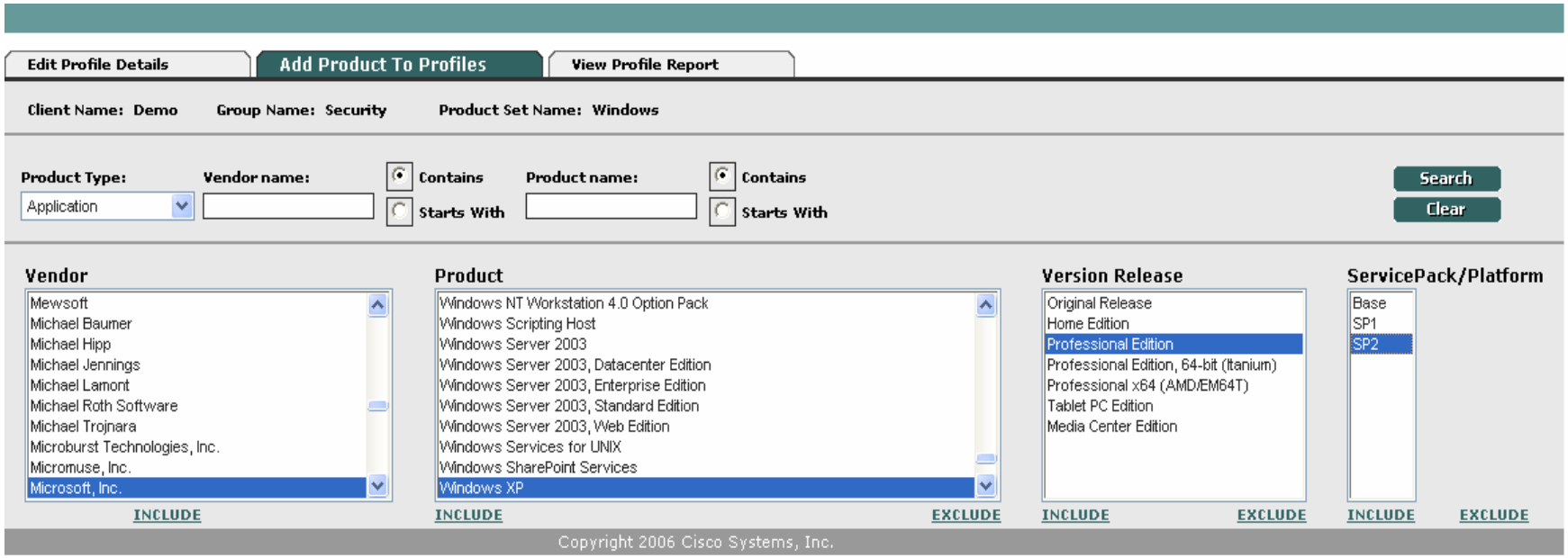
- Comprehensive threat and vulnerability database
- User-defined technology profiles
- Customized notifications
- Tasking and workflow management
- Cisco IPS Signature correlation
- Optional XML Feed

IntelliShield Database



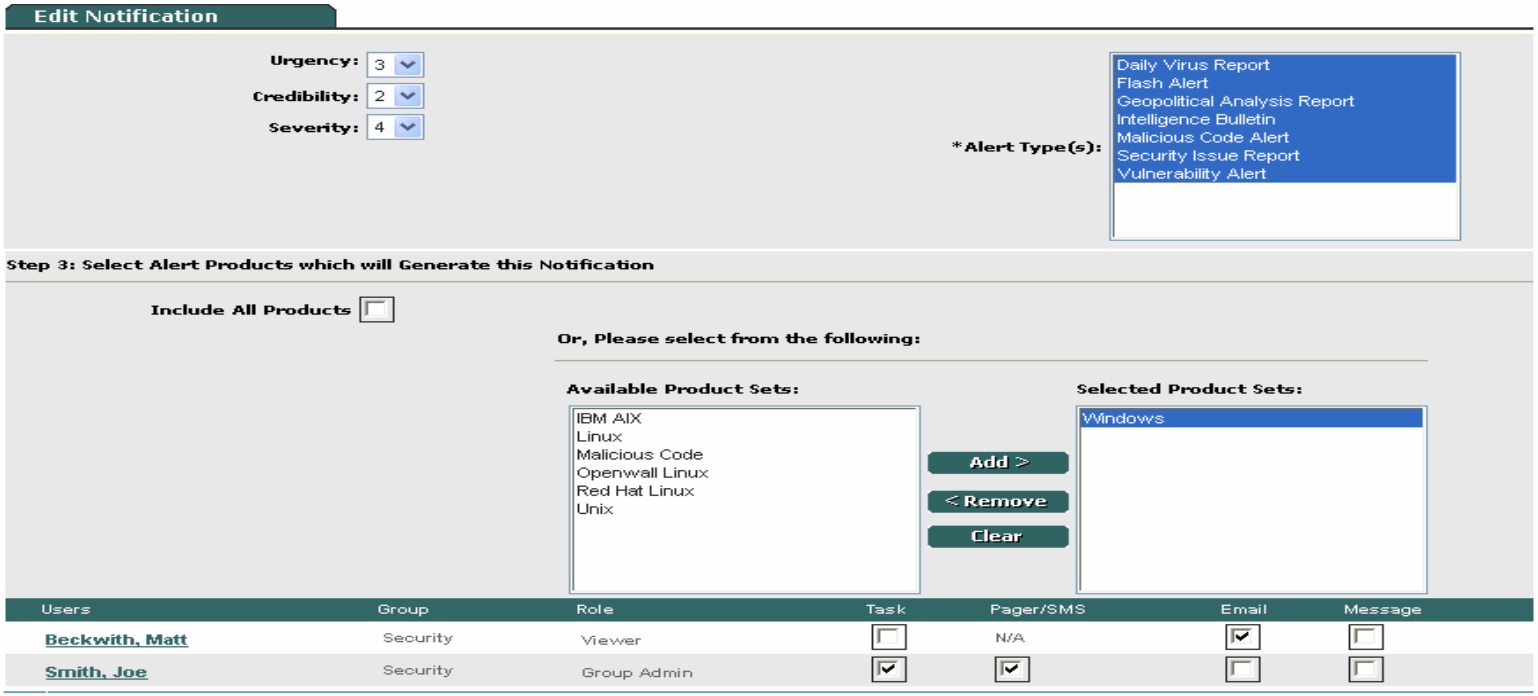
- Access to over 14,000 Alerts dating back to May of 2000
- Advanced search feature allows clients to perform in-depth research and analysis

User-Defined Technology Profiles



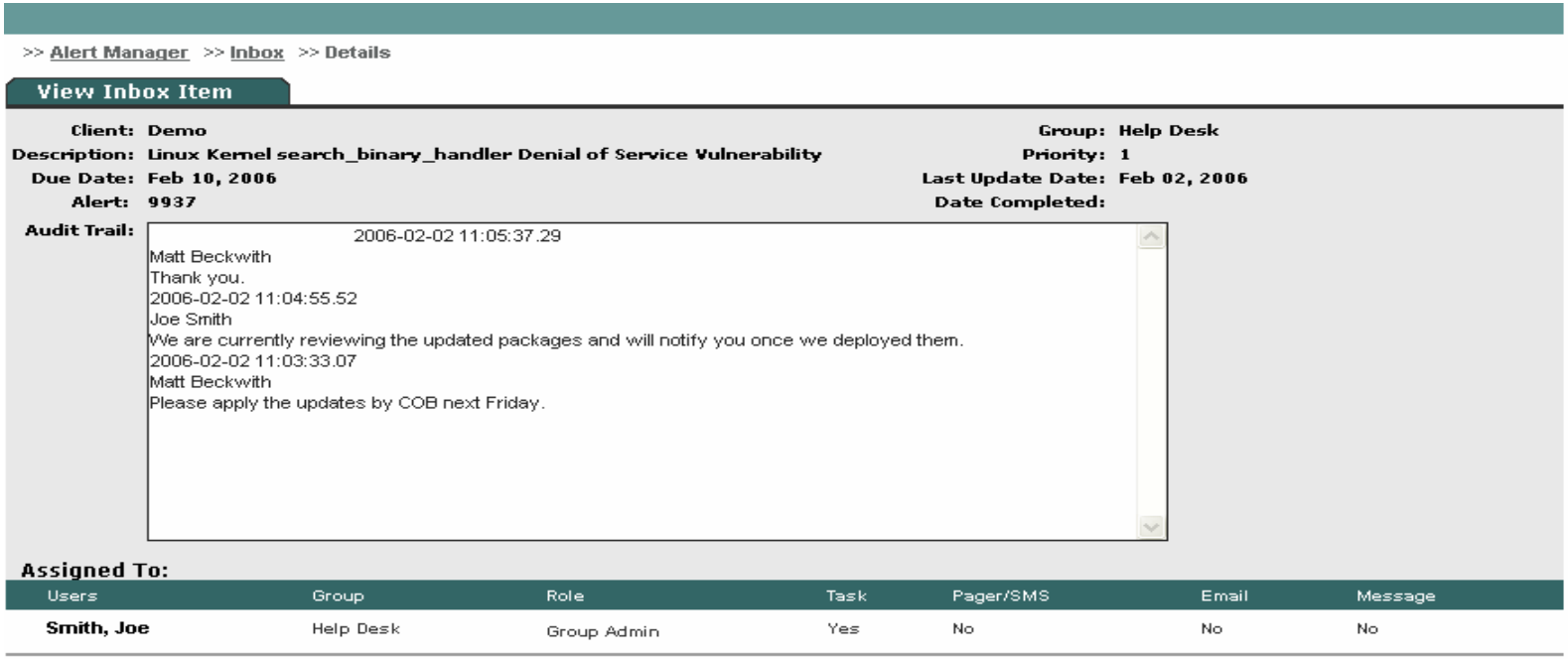
- Create product sets based on technologies relevant to your infrastructure
- The ability to customize at different levels—vendor, product, version, or service pack

Customized Notifications



- 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



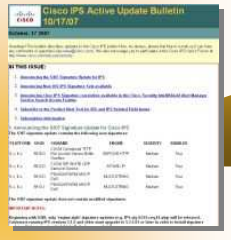
- Assign tasks to individuals and share critical information across the enterprise
- View what tasks are outstanding, who is assigned each task, as well as the current status of remediation efforts

Cisco IPS Signature Correlation With IntelliShield Alerts

Security Intelligence Services

IntelliShield Alert Manager

IntelliShield Alerts for new Vulnerabilities



IPS Signature Updates

Cisco Services for IPS

Comprehensive support for Cisco IPS solutions combining signature file updates with SMARTnet

IPS Signature Correlation with IntelliShield Alerts

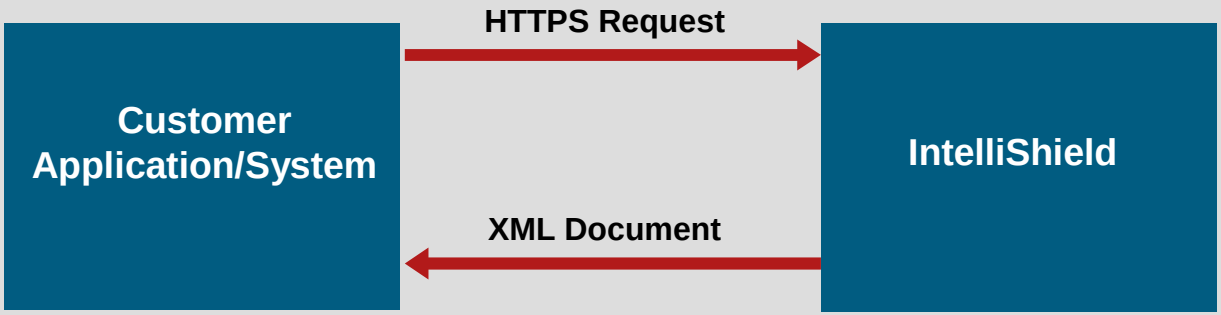
- **Access the latest vulnerabilities and threats with correlated Cisco IPS Signature information: signature name, signature ID, release version, and release date**

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**

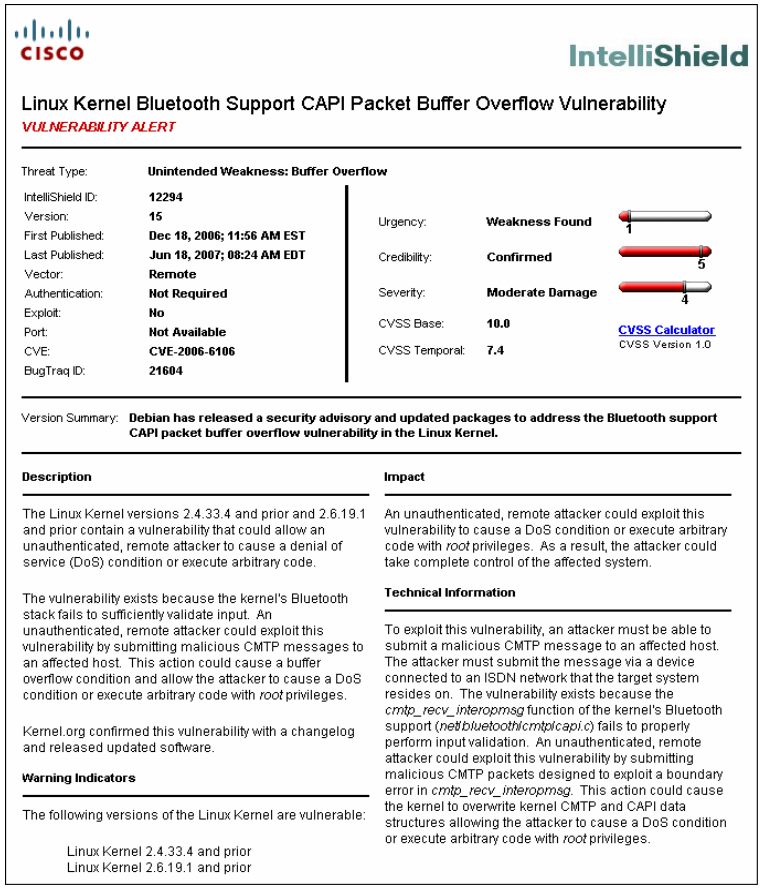
IntelliShield Alert Manager XML Service

- 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



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 CMTP 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.

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

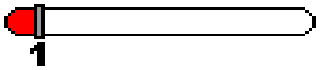
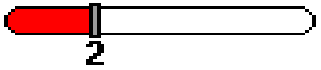
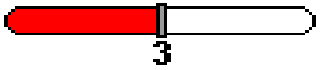
Impact

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

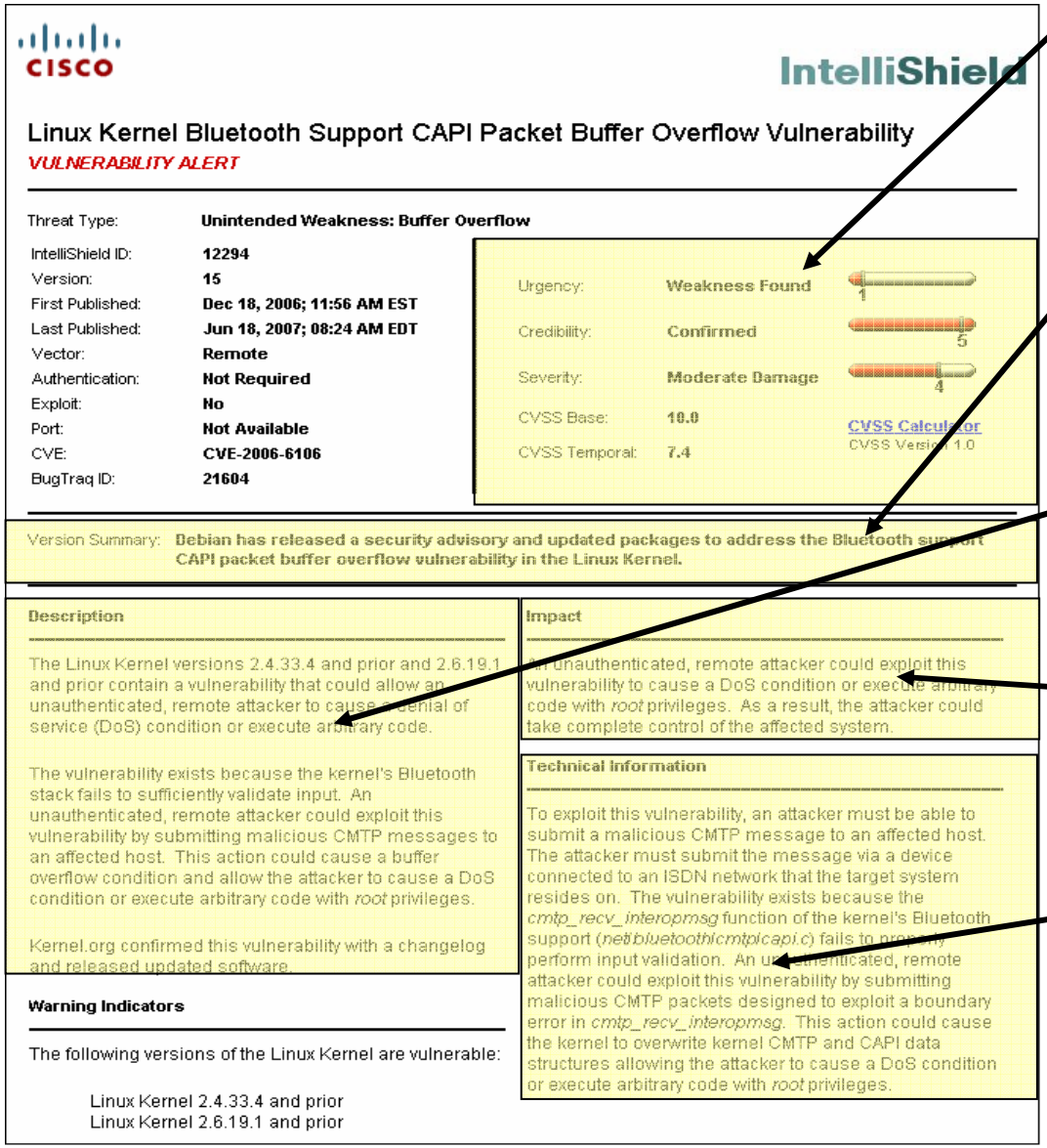
To exploit this vulnerability, an attacker must be able to submit a malicious CMTP message to an affected host. The attacker must submit the message via a device connected to an ISDN network that the target system resides on. The vulnerability exists because the *cmtp_recv_interopmsg* function of the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

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 CMTP 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 CMTP 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\cmtp\capi.c*) fails to properly perform input validation. An unauthenticated, remote attacker could exploit this vulnerability by submitting malicious CMTP packets designed to exploit a boundary error in *cmtp_recv_interopmsg*. This action could cause the kernel to overwrite kernel CMTP 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

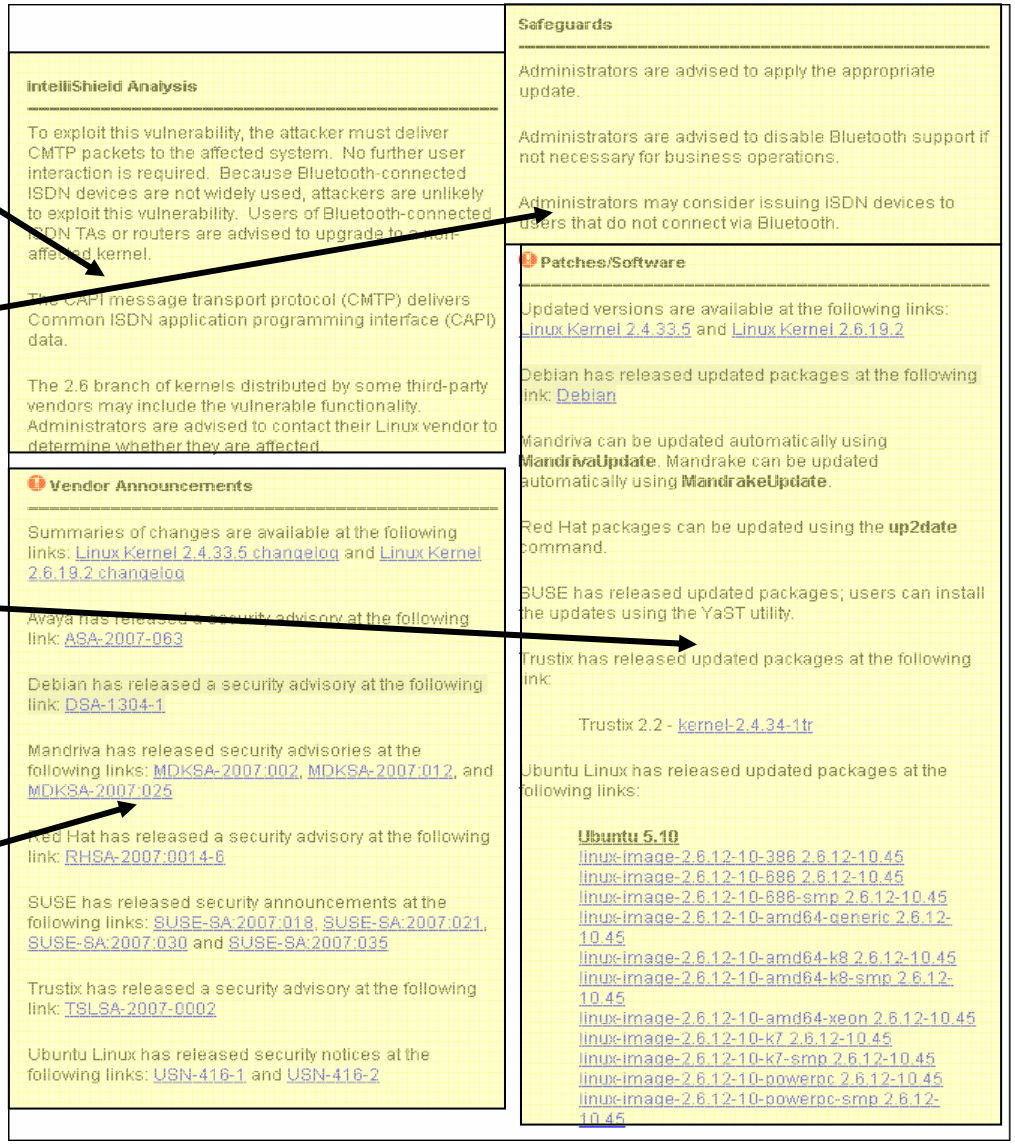
Workarounds and mitigation information

Patches/Software

Applicable patches and software available for download

Vendor Announcements

Links to associated vendor advisories



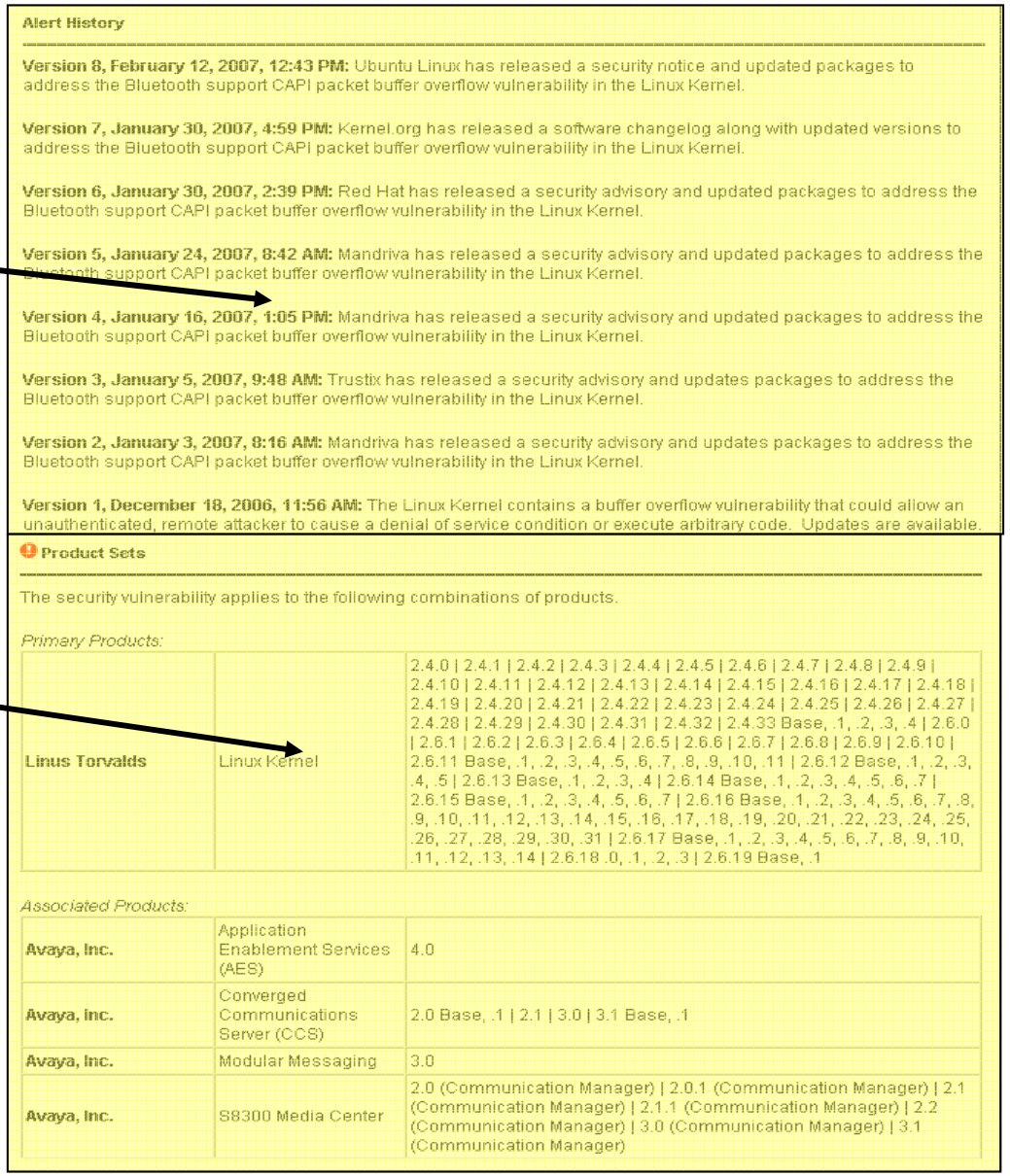
“Filtered” Intelligence

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:

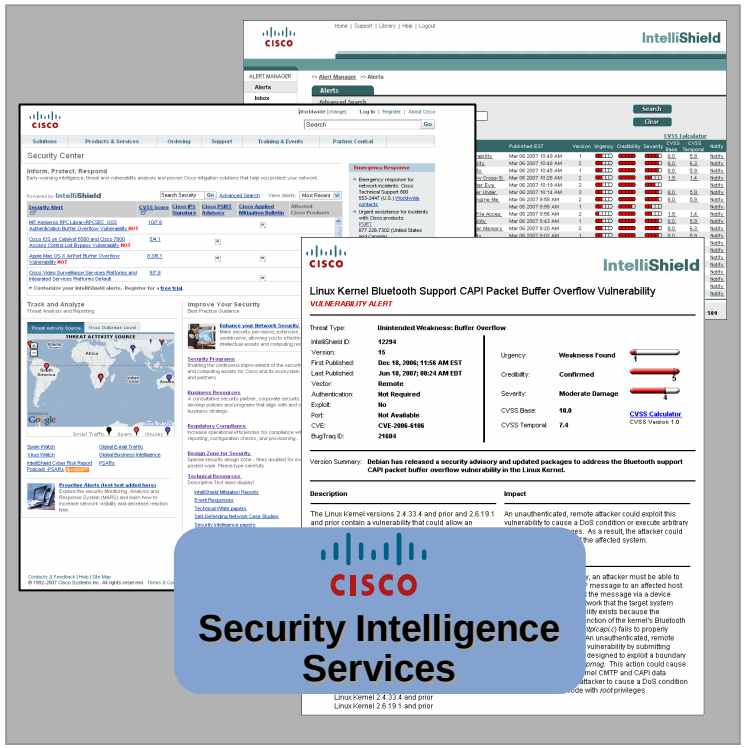
Linus Torvalds	Linux Kernel	2.4.0 | 2.4.1 | 2.4.2 | 2.4.3 | 2.4.4 | 2.4.5 | 2.4.6 | 2.4.7 | 2.4.8 | 2.4.9 | 2.4.10 | 2.4.11 | 2.4.12 | 2.4.13 | 2.4.14 | 2.4.15 | 2.4.16 | 2.4.17 | 2.4.18 | 2.4.19 | 2.4.20 | 2.4.21 | 2.4.22 | 2.4.23 | 2.4.24 | 2.4.25 | 2.4.26 | 2.4.27 | 2.4.28 | 2.4.29 | 2.4.30 | 2.4.31 | 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

Associated Products:

Avaya, Inc.	Application Enablement Services (AES)	4.0
Avaya, Inc.	Converged Communications Server (CCS)	2.0 Base, .1 | 2.1 | 3.0 | 3.1 Base, .1
Avaya, Inc.	Modular Messaging	3.0
Avaya, Inc.	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)

Cisco Security IntelliShield Alert Manager Summary

- Market leading security intelligence
- Reduce costs of patching and remediation
- Sign up for a 6-month trial today



For a 6-month trial
www.cisco.com/go/intellishield/trial

Cisco Security Center
www.cisco.com/go/security