



X-Force[®] Threat Insight Quarterly

Voice over Internet Protocol (VoIP) — Transforming Business, Inviting Attack

May 2005

 **INTERNET | SECURITY | SYSTEMS[®]**
Ahead of the threat.[™]

Contents

Introduction	1
Focus Topic - VoIP	2
Conclusion	4
Other Significant and Prolific Issues within Q1 2005	5
Future Topics for 2005	7
References	7
About Internet Security Systems	8

Introduction

Voice over Internet Protocol or Voice over IP (VoIP) is one of the technologies vigorously being adopted by businesses around the globe. According to Gartner, spending by US companies and public-sector organizations on VoIP systems will grow to \$903 million in 2005; this was up from the \$686 million noted in 2004. By 2007 Gartner expects 97 percent of new phone systems installed in North America to be VoIP or hybrids. The Telecommunication Industry Association predicts that 26 million users will have VoIP by 2008.

With the growing prevalence and dependence on VoIP today, security professionals must view this as a critical component of their network topology and afford it the appropriate protection and attention. This report is intended to arm security professionals with the essential knowledge needed to identify the security risks associated with VoIP.

Additionally, this report will highlight some other challenges faced by security professionals throughout the first quarter of 2005.

About this report

The X-Force Threat Insight Quarterly (Threat IQ) is designed to highlight some of the most significant threats and challenges facing security professionals today. This report is a product of ISS' Managed Security Services and is compiled by ISS' X-Force security intelligence team. Each issue will focus on a specific challenge and provide a recap of the most significant recent online threats.

ISS' X-Force is a primary security research organization that discovers vulnerabilities and security flaws in computer networks and tracks emerging Internet threats. The ISS X-Force serves as trusted security advisor to the U.S. Department of Homeland Security as well as many other federal, state and local government organizations, helping create governmental security standards and initiatives.

X-Force research forms the basis for ISS' Proventia® Enterprise Security Platform (ESP). By researching vulnerabilities, ISS is able to update its products and services to prevent attacks before they negatively impact an organization. All ISS products and services rely on X-Force research to preempt threats.

Questions or comments regarding the content of this report should be addressed to X-ForceThreatIQ@iss.net.

Voice over IP (VoIP) — Transforming Business, Inviting Attack

Modern society takes some things for granted, believing they are a constant. Emergency Services like the 911 system is a perfect example. But what if you dialed 911 and no one answered, and the reason was because you simply could not get through?

A variety of scenarios could ensue including loss of life, buildings, and inventory. What if the call center you were dialing from was dependent on VoIP and had been brought down by a targeted denial of service (DoS) attack using VoIP Spam? You would be unable to reach the neighboring Emergency Service center. Now that VoIP is becoming such a prevalent communications technology, concerns of an attack against the technology are warranted.

What if the same scenario were to happen to a business call center, which provides technical support, sales and internal communications? The financial losses could be unrecoverable. VoIP technology is becoming as much a part of the corporate networking environment as Web servers, e-mail and databases. Already, a significant amount of emphasis is placed on these critical systems, from the operating system (OS), to the applications, to ensuring adequate network bandwidth to support business requirements. Has the same vigilance and attention been afforded to ensure that your VoIP communications are equally planned, protected and maintained?

What is VoIP?

The concept of Voice over IP (VoIP) is relatively simple - VoIP allows you to make phone calls over the Internet, using it as a transmission medium rather than the traditional circuit transmissions of the Public Switched Telephone Network (PSTN). The technology behind VoIP, however, is a complex collection of protocols, applications and appliances that all require attention when planning a new implementation or conducting risk assessments of existing technology.

Exposures and Security Threats

Exposures and security threats to VoIP can be broken down into two main categories. The first category is generic to the individual systems and components that VoIP technology relies on — namely the systems and servers. The second category includes those threats and exposures specific to the VoIP technology itself.

Because VoIP travels over the network and the Internet, it is susceptible to the same security perils that reside in the various components from which the network and network traffic are composed. This includes e-mail, software, network and IP protocols (H.323, SIP, RTP, TCP/UDP, etc.), weak server configurations, operating system based flaws, inadequate firewall rules or poor security practices (weak passwords, permissions, etc). Thus, VoIP may be open to several types of attacks such as a man-in-the-middle, DoS or data injection. Successful

Where did VoIP come from?

Voice over Internet Protocol (VoIP) is often referred to as a new technology. However, the emphasis on producing the IP-based solution was developed in the early 90s. Rather, what's new is the introduction of specialized devices and applications that can contain their own security ramifications.

Many applications and devices fully support VoIP integration into traditional network data streams. One of the first applications developed was an Internet phone introduced in 1995 by VocalTec, an Israeli company. Since then, several vendors have produced devices which support both traditional data-driven network traffic and VoIP.

The vigorous induction of VoIP into the corporate network has been fostered not only by the increased production of inexpensive technology solutions, but by the general ease of use the solutions provide. However, those who intend to enable VoIP on their network should note that VoIP developers were not as focused on security in the early 90s as we are today; thus the protocols and technologies utilized by VoIP were not developed with a preemptive security model in mind.

exploitation could grant a hacker the ability to hijack an individual's credentials, "spoof" their caller ID, or take down an entire call center.

These attacks could originate via the local network or remotely, depending on the attack vector chosen. It is important to recognize that in the event of a significant network-based attack, it is not only the integrity of the network at risk but the entire communications infrastructure. The level of integration these components could have in a given corporate network environment provide compelling reasons to specifically address VoIP within your network security assessment strategy and processes.

In addition to the exposures and threats inherent to networked systems, VoIP introduces added risks that must be taken into account. ISS' X-Force Threat Analysis Service has covered a number of flaws affecting VoIP within the Daily Assessment featured on the service's Web site. A vulnerability in Avaya's IP Office Phone Manager was highlighted on February 23rd, as was the exploit code subsequently published 48 hours later. The number of VoIP-related vulnerabilities is expected to move in lock step with the projected growth of the market's demands.

Over the past few years, a few vulnerabilities have surfaced affecting either the devices and/or protocols that support VoIP data transmissions. A well-known example was featured in an alert published by ISS' X-Force on January 13, 2004. The alert provided information regarding numerous vulnerabilities, affecting H.323-based VoIP products. The discovery was made through a suite of testing tools developed by Finland's University of Oulu that targeted products using the H.323 call-signaling protocol. The H.323 protocol most commonly supports VoIP and video conferencing applications. ISS' X-Force developed seven separate checks for this disclosure alone. As the technology becomes more prevalent, the focus on discovering vulnerabilities such as those uncovered by the University of Oulu will become increasingly concentrated — opening up the average corporation to higher risk.

Breaches of Confidentiality and Fraud

As with most network security issues, the degradation of confidentiality, integrity, and availability are the three most significant threats facing those utilizing VoIP. One of the differentiators between VoIP and its physical counterpart is that an attacker could essentially be anywhere in the world. VoIP does not require physical access to a device located on the targeted corporation's network to tap into, disrupt, drop, hijack and/or eavesdrop on a transmission. These are only a few of the incidents that could impact a VoIP call.

Inherent flaws associated with the various VoIP protocols could be utilized to execute a phishing attack, DoS or data corruption, and could lead to other forms of fraud and/or identity theft. H.323 is

just one of a number of protocols utilized by VoIP. Each protocol, such as H.225, Session Initiation Protocol (SIP), Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NATs)-(STUN), Q.931, H.245 and T.120, presents its own unique flaws and security challenges.

In the last X-Force Threat IQ, we focused on phishing, the growing threat associated with identity theft and loss of personal information. VoIP provides with yet another avenue of opportunity for phishers to gain personal information like Social Security Numbers or banking transaction data.

For those interested in learning more about VoIP related protocols, the reference section near the conclusion of this report features a number of links which cover a wide range of associated topics.

Challenges and Solutions

The security model for VoIP adopted by many organizations relies on security by obscurity; providing VoIP protection by using methods of bandwidth management including traffic shaping, rate limiting or quality of service (QoS). The fundamental discrepancy in this security model is that the same techniques employed to protect are also used in service delivery. This could lead to degradation of QoS. It is also likely that a hacker would craft an attack with this type of model in mind.

VoIP brings to market financial incentives and ease of use that continue to draw interest, pushing it further and further into mainstream communications. All of which contribute to its appeal within the hacker underground, thus leading to a future of targeted research and attacks.

Whether you're reviewing the security of an existing VoIP implementation or considering the impact of employing this technology in your organization, you should formulate a well-contemplated assessment plan. This should involve a security team with forethought and a strong grasp of the technology as a multi-layered threat, which requires a multi-layered security solution.

What should my VoIP security solution provide?

An ideal VoIP security solution would provide blended preemptive protection from both the threats which affect the traditional data-driven network traffic and also the underlying infrastructure, devices and protocols that support VoIP data transmissions. Keep in mind that this protection should not interfere with the devices providing QoS assurance.

To combat and give adequate visibility into this emerging threat, consider deployment of a network intrusion prevention system (IPS). Additionally, regular penetration tests targeting VoIP and other critical network assets will assist in identifying exposures and the type of implementation or countermeasures correct for the network.

It can also assist in defining an escalation process and procedures for handling security incidents. Combined, these measures ensure your organization possesses a well-designed security posture containing the right type of resources and bandwidth capabilities to circumvent attacks such as a DoS.

Your organization could also consider deploying a separate Local Area Network (LAN) as an alternative to a fully integrated network, to reduce crossover compromise. Of course, this may dilute the cost benefits associated with deploying VoIP as the increased infrastructure costs would offset some of the gains.

It is also important to keep in mind that many VoIP communication providers offer voice and call-control encryption over the IP LAN or Wide Area Network (WAN). Verify that the providers you are considering offer this service.

Conclusion

The previous X-Force Threat IQ introduced the growing affiliation between phishers, fraudsters and organized crime syndicates. This trend shows no signs of slowing. Each new layer of technology that corporations use daily adds to the plausibility of compromise and loss of integrity; all leading to grey areas of security. Just imagine how difficult it would be to determine if a call was actually legitimate. What if a hacker could appear to be calling from your banking institution?

Multi-layered platforms, the development of new software/appliances and the overall lack of integrated security leave the VoIP attack vector smoldering like a volcano. As the pressure mounts towards integrating the technology into mainstream business and producing new applications and devices, the attack vector swells. The trick is to ensure that the security solutions adopted never allow any one situation to reach a critical level.

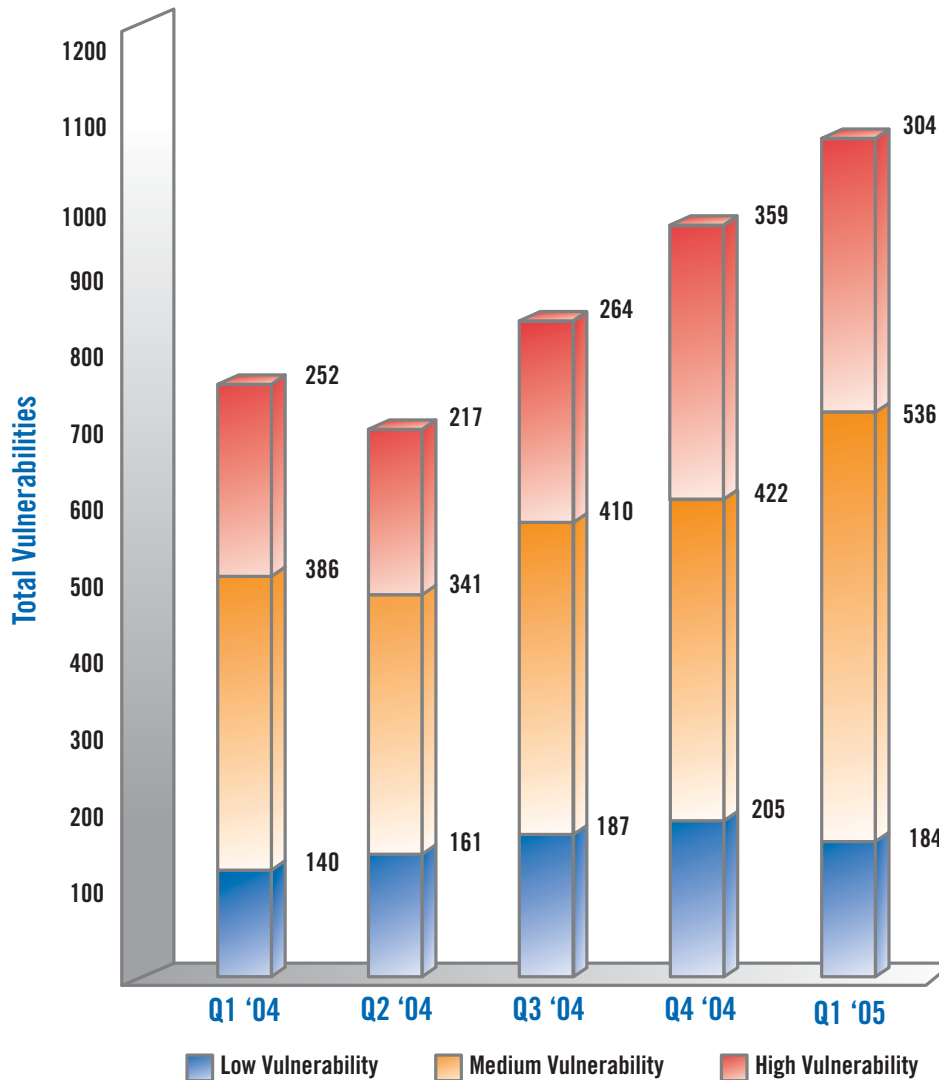
The appropriate solution does not necessarily have to come from within your organization. Contacting a consulting service or managed service provider as the source of deployment and risk management may enable your organization to continue reaping the benefits of VoIP without accruing unnecessary overhead

What things should I keep in mind to mitigate risk?

- *Be sure to enable as many of the security features available as are plausible, being careful to consider the impact various “features” will have on the overall QoS.*
- *During the initial selection process, be sure to choose security products that are considered VoIP-aware, such as perimeter firewalls which support application layer gateway technology. Verify that they dynamically open and close ports for voice traffic..*
- *Implementing a strong authentication and encryption posture is key to ensuring the integrity of both the network infrastructure and VoIP communications. Leverage lessons learned while developing the processes and procedures for network security, as many are of great assistance and transferable to the VoIP implementation or assessment*
- *Ensure access controls are in place to authenticate users of VoIP infrastructure.*
- *Consider deploying a Virtual Private Network (VPN) and/or utilizing the Extensible Authentication Protocol (EAP) for additional security measures.*
- *Utilize private VPN connections for point to point voice communication within WAN.*
- *Utilize some of the same security methodologies as applied to IP assignments such as applying ingress and egress filters to the Call source addresses.*
- *Use host-based and gateway anti-virus protection to protect critical VoIP servers*
- *Become familiar with the more popular protocols to develop a knowledgeable understanding of how the applications utilizing the protocols will interact with other security assets such as firewalls.*

Other Significant and Prolific Issues within Q1 2005

In first quarter of 2005, Internet Security Systems' X-Force analysts researched and assessed 1,024 security-related threats. The independent research, development and monitoring conducted by our X-Force analysts directly contributed to the continuous and preemptive protection provided to the ISS customer base. During the first quarter of 2005, ISS' X-Force research and development analysts independently discovered security issues leading to five security advisories and two security alerts regarding various underlying threats. This section of the report features some of the more significant threats of first quarter 2005.



ISS X-Force Database

AntiVirus Library

The X-Force research and development team discovered significant flaws within four major antivirus vendors' security applications, in which each is susceptible to an overflow within various components of the process transporting the antivirus library. If a hacker were to successfully exploit these vulnerabilities, the hacker could gain unauthorized access to the networks and machines being protected by the various vendors' antivirus library products. It is also important to note that an attacker requires no authentication to utilize any vulnerability, which could lead to system or network compromise. ISS' X-Force shipped preemptive protection and worked closely with Trend Micro, F-Secure, Symantec and McAfee to ensure protection was provided for all affected products.

Mozilla Foundation GIF Overflow

On March 23rd, the ISS X-Force released an advisory defining a flaw discovered by X-Force in the GIF image processing library used in software developed by the Mozilla Foundation. The library is used by the Firefox Web browser, the Mozilla browser, and Thunderbird Mail client. The flaw can be utilized to generate a heap overflow within the application viewing the image, which could lead to arbitrary code execution and remote compromise. If an attacker were to successfully exploit the vulnerability and cause a heap overflow, they could gain access to confidential information and infiltrate other portions of the network. However, it is important to note that successful exploitation requires user interaction. The user would have to view a Web site or e-mail containing the maliciously crafted image.

The time frame between the publication of a vulnerability and the release of malicious exploit code is often referred to as the “patching window.” This “window” reflects the amount of time security teams have to identify vulnerable systems and either apply a vendor patch or employ some remediation measure such as a firewall or intrusion prevention system blocks. The fact that this window had drastically reduced was highlighted in the previous X-Force Threat IQ report, which covered some of the significant threats of 2004. In 2005, the “window” has become almost non-existent, as evident by the specific examples outlined here.

Microsoft Security Releases

On January 11th, Microsoft released Security Bulletins MS05-001 “Vulnerability in HTML Help Could Allow Code Execution (890175) (Critical),” MS05-002 “Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (891711) (Critical)” and MS05-003 “Vulnerability in the Indexing Service Could Allow Remote Code Execution (871250) (Important).”

Within less than 48 hours, a proof-of-concept exploit and Trojan, Backdoor.Globe, was released for the vulnerability addressed in the Microsoft Security Bulletin MS05-002. Exploit code was made publicly available in late December 2004 for the vulnerability detailed in MS05-001.

In the February Microsoft Security Bulletin release, several threats were identified. The most notable risks were associated with the vulnerabilities disclosed in MS05-010 and MS05-011, which address network-based remote compromise issues in the SMB client and in the License Logging Service. A remote attacker could potentially gain complete control over affected systems or run arbitrary code by exploiting said vulnerabilities.

These were just two of twelve Microsoft security bulletins that covered sixteen separate issues published within the February release. Proof-of-concept/exploit code has since been released for both MS05-005 and MS05-009. We advised that those who wish to apply all of the Microsoft patches remember to utilize both the Windows and Office Update.

VERITAS Backup Exec Name Service Exploitation

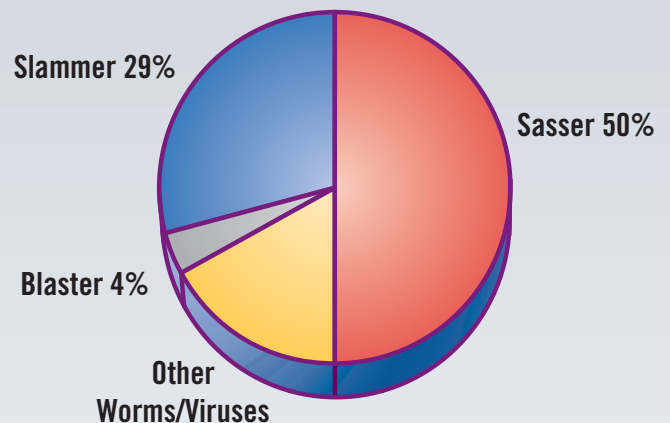
An increase in port scans targeting TCP port 6101 was noted across multiple infrastructures in mid-January. Investigation into the traffic revealed that there was an association with a VERITAS Backup Exec Name Service vulnerability, announced in December 2004 (CAN-2004-1172), and newly released exploit code. Internet Security Systems' X-Force Threat Analysis Service (XFTAS) featured information on the vulnerability and exploitation in its Daily Assessment Summary. Additionally, reports of similar activity had been noted on various security news publications, mailing lists and Weblogs.

Multiple Vulnerabilities in Cisco IOS

ISS' X-Force released an alert in January outlining the risks associated with vulnerabilities discovered in Cisco's Internetwork Operating System (IOS). Cisco released three advisories outlining various issues on January 26th: “Multiple Crafted IPv6 Packets Cause Reload,” “Crafted Packet Causes Reload on Cisco Routers” and “Cisco IOS Misformed BGP Packet Causes Reload.” The ISS X-Force Alert specifically focused on the Internet Protocol version 6 (IPv6) and Border Gateway Protocol (BGP)-related threats. It is important to note that the BGP vulnerability requires the “bgp log-neighbor-changes” option to be enabled. Although this is not a default setting and may be perceived as a mitigating factor, it is commonly enabled to perform system diagnostics. This alert was later updated to reflect new information uncovered by ISS' X-Force research and development analysts. Our analysts uncovered that the vulnerabilities could allow a remote attacker to compromise a Cisco router or cause OS reloads. Additionally, a long-term DoS condition could be created if the OS reloads were caused in succession. Upon successful exploitation, the attacker could gain full control of an affected router.

Though specific exploit code regarding the Cisco vulnerabilities has not yet been noted, the emergence of threats taking advantage of IPv6 settings is of concern and worth adding to security assessments of networking devices shipping with “IPv6-aware” features.

Notorious Worms Still Threaten Unprotected Systems



These numbers includes new variants or worms utilizing these infamous vulnerabilities

ISS Managed Security Services' X-Force Protection System collects and analyzes approximately 50 million IPS/IDS log events a day from devices located across the globe. Approximately 15% of the traffic recorded during the first quarter of 2005 was worm- and virus-related activity. Many of the vulnerabilities bundled in such notorious worms as Sasser, Slammer and Blaster were repackaged in other worms and exploits such as Mytob, Korgo, Gaobot, Spybot, Kelvir, Backdoor.IRC.Cirebot, and Hacktool.LsassSba. Unpatched and/or infected systems on the Internet still present a threat to Corporate networks two years after these vulnerabilities were first published.

Future Topics for 2005

The threats described in this report are but a sample of the challenges facing corporate security teams. Because education is a key defensive element, ISS is committed to producing similar reports like this one on a quarterly basis. Future topics will include:

Trojans, Spyware and Adware

IPv6 Protection

Wireless/Cellular Security

References

Educational Material

VoIP

<http://www.webopedia.com/TERM/V/VoIP.html>

How Virtual Private Networks Work

<http://computer.howstuffworks.com/vpn.htm>

EAP

<http://www.webopedia.com/TERM/E/EAP.html>

LAN

http://www.webopedia.com/TERM/I/local_area_network_LAN.html

WAN

http://www.webopedia.com/TERM/W/wide_area_network_WAN.html

VoIP Spam – SPIT (Spam over internet telephony)

[http://en.wikipedia.org/wiki/Spit_\(VoIP_spam\)](http://en.wikipedia.org/wiki/Spit_(VoIP_spam))

<http://www.webopedia.com/TERM/s/spit.html>

VoIP spam—it's coming

<http://www.voip-news.com/art/4e.html>

Net phone customers brace for 'VoIP spam'

http://news.zdnet.com/2100-9584_22-5302988.html

VoIP Protocols:

<http://www.protocols.com/pbook/VoIP.htm>

<http://www.protocols.com/pbook/VoIPFamily.htm>

Statistics and Breakout Boxes

Corporate VOIP spending to reach \$903 mln in 2005:

<http://www.itfacts.biz/index.php?id=P2656>

History of Voice Over IP:

<http://www2.rad.com/networks/2001/voip/history.htm>

VoIP Phone Systems Introduction:

<http://smallbusiness.yahoo.com/resources/article.php?mcid=5&scid=49&aid=627>

The Third Age Of VoIP: Embracing Real-Time Call Control:

<http://www.telic.net/thirdage.htm>

Advisories and Alerts Referenced

Alerts:

Multiple Vulnerabilities in Microsoft Products – February 2005 – (February 08, 2005)

<http://xforce.iss.net/xforce/alerts/id/186>

Multiple Vulnerabilities in Cisco IOS – (January 27, 2005)

<http://xforce.iss.net/xforce/alerts/id/185>

Multiple Vendor H.323 Implementation Vulnerabilities – (January 13, 2004)

<http://xforce.iss.net/xforce/alerts/id/160>

Advisories:

Mozilla Foundation GIF Overflow – (March 23, 2005)

<http://xforce.iss.net/xforce/alerts/id/191>

McAfee AntiVirus Library Stack Overflow – (March 17, 2005)

<http://xforce.iss.net/xforce/alerts/id/190>

Trend Micro AntiVirus Library Heap Overflow – (February 24, 2005)

<http://xforce.iss.net/xforce/alerts/id/189>

F-Secure AntiVirus Library Heap Overflow – (February 10, 2005)

<http://xforce.iss.net/xforce/alerts/id/188>

Symantec AntiVirus Library Heap Overflow – (February 08, 2005)

<http://xforce.iss.net/xforce/alerts/id/187>

Additional References

X-Force Threat Insight Quarterly (Threat IQ): Phishing and other significant threats of 2004:

http://documents.iss.net/ThreatIQ/ISS_XFIQ0205.pdf

ISS' X-Force Threat Analysis Service

<http://xforce.iss.net/xftas/>

X-Press Updates™:

<http://www.iss.net/xpu/>

Choose Effective VoIP Security Solutions:

<http://www.iss.net/resources/voip.php>

Choose an Effective Network Intrusion Prevention System:

http://www.iss.net/resources/choose_an_IPS.php

Internet Security Systems X-Force Alerts and Advisories:

<http://xforce.iss.net/xforce/alerts>

X-Force Catastrophic Risk Index (CRI) – an up-to-date list of the most serious, high-risk vulnerabilities and attacks. Developed by the X-Force, the CRI enables cost effective and proactive protection around threats and vulnerabilities that pose the greatest risk to confidentiality, integrity and availability of critical business systems and applications:

<http://xforce.iss.net/xforce/riskindex/>

Avaya IP Softphone plaintext password:

<http://xforce.iss.net/xforce/xfdb/19438>

Avaya IP Office Phone Manager Local Passwords Disclosure Exploit:

<http://www.k-otik.com/exploits/20050224.avaya.cpp.php>

Article: VoIP Security Alliance launched:

<http://www.techworld.com/mobility/news/index.cfm?NewsID=3088&Page=3&pagePos=20>

About Internet Security Systems

Internet Security Systems is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. ISS products and services are based on the proactive security intelligence conducted by ISS' X-Force research and development team – the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call **800-776-2362**.