An X-Force™ Guidelines Document

INTERNET
SECURITY
SYSTEMS™

X-Force™ Vulnerability Disclosure Guidelines

(Revised November 18, 2002)

6303 Barfield Road • Atlanta, GA 30328 Tel: 404.236.2600 • Fax: 404.236.2626

Introduction

Internet Security Systems (ISS)' ***X-Force™*** organization is a leading research and development group dedicated to discovering vulnerabilities and design weaknesses that potentially open operating systems and applications to attack or misuse. This process includes both active research of products and technologies and ongoing surveillance within the hacking underground. Relevant discoveries are released in the form of alerts and advisories, and are delivered within product enhancements for Internet Security Systems' enterprise prevention and protection platform, in order to protect Internet Security Systems' customers, critical infrastructure and the Internet at large.

The following X-Force Disclosure Guidelines communicate X-Force policies and procedures concerning the disclosure of vulnerability information to third-party vendors and the general public. These standards provide a careful balance between sometimes conflicting interests and are intended to be as reasonable and fair as possible to all parties involved.

These guidelines may change from time to time, and Internet Security Systems, Inc. disclaims any obligation to provide notice of changes. Revised guidelines will bear a new revision date.

Definitions

- **X-Force™ Security Advisories** – X-Force Security Advisories contain information from original, internal research. An advisory includes a synopsis of the security vulnerability, information on impact of the discovered issue, a listing of affected versions, a detailed description of the issue, recommendations for managing and/or correcting the issue, and other relevant/additional information. All X-Force Security Advisories are released on the ISS Web site at http://xforce.iss.net/alerts for public viewing and are announced by an X-Force Security Brief.

- **X-Force™ Security Alerts** – Security Alerts are released when X-Force discovers additional information about an existing security issue. The security information in Alerts is released in accordance with the Disclosure Guidelines procedures. All X-Force Security Alerts are released on the ISS Web site at http://xforce.iss.net/alerts for public viewing and are announced by an X-Force Security Brief.

- **X-Force™ Security Briefs** – The ISS X-Force Security Brief is a less detailed version of a Security Advisory or Alert. It contains a synopsis of the issue, and affected versions. This document is publicly distributed by email to various mailing lists. An electronic link to the complete, corresponding X-Force Security Advisory or Alert is included.

- **X-Force™ Threat Analysis Service (XFTAS)** – The X-Force Threat Analysis Service (XFTAS) enables active security management through comprehensive evaluation of global online threat conditions and detailed analyses tailored for specific customer needs. X-Force Threat Analysis Service blends threat information collected from Internet Security System's international network of Security Operations Centers and trusted security intelligence from the X-Force research and development organization. This powerful combination clearly illustrates the nature and severity of Internet threats. Daily summaries provide current and forecast assessments for active vulnerabilities, viruses/worms and threats, including links to recommended fixes and security advice.

  Internet Security Systems' XFTAS is a fee-based subscription service that contains proprietary information from Internet Security Systems. The information disseminated by the service is also considered confidential and proprietary to Internet Security Systems, and is licensed to subscribers only. Subscribers are not permitted to re-distribute the information outside of the parameters outlined in the subscriber's XFTAS terms and conditions with Internet Security Systems.

X-Force develops checks and signatures for Internet Security Systems' products. If possible and applicable, a procedure to detect and block the vulnerability through the use of Internet Security Systems' prevention and protection products and services will be recommended in a Security Brief made available through the XFTAS.

- **Internet Security Systems X-Force™ Organization** – Internet Security Systems' X-Force organization is a leading group of security experts dedicated to active intelligence collection and analysis leading to public education against online threats. The X-Force identifies, assesses, and tracks the evolution of threats using the latest equipment and lab facilities including ISS' Global Threat Operations Center (GTOC) where the severity of Internet threats and vulnerabilities is monitored 24 hours a day.

  The research conducted by the X-Force is made available to the public through X-Force Security Briefs, and are accompanied by protection strategies in accordance with the X-Force Disclosure Guidelines. The X-Force staff possesses a wide range of expertise in security management strategies and tactics. This deep understanding of distributed computing, global networking, programming and forensics contributes to the credibility and integrity of their research, and keeps them at the forefront for combating the latest developments in online security.

Vulnerability Disclosure Process

Internet Security Systems' X-Force engages in active programs of original Internet and network security research. The disclosure of vulnerability information is provided as a public service to vendors, Internet Security Systems' customers and the general public. The X-Force vulnerability disclosure process is divided into four stages:

I. Initial Discovery Phase
II. Vendor Notification Phase
III. Customer Notification Phase
IV. Public Disclosure Phase

When a vulnerability is discovered, X-Force uses the following procedures for initial discovery, notification and public disclosure:

I. Initial Discovery Phase

X-Force Researchers discover and confirm a security vulnerability. The security vulnerability is documented in a draft X-Force Security Advisory and an X-Force Security Brief is created from a subset of the Advisory.

II. Vendor Notification Phase

- X-Force establishes initial communication with the affected vendor.

  - X-Force defines a vendor as any company, group, or organization that develops and provides software, hardware, or firmware applications, either for sale or as part of a free distribution.

  - X-Force defines initial communication as any attempt to contact the vendor via e-mail and/or telephone, either through pre-established relationships, through publicly available contact information published within the vendor's Web site or sales collateral.

- X-Force notifies the vendor of the discovery of a vulnerability and that X-Force will privately and publicly distribute critical information on the schedule outlined in this document. X-Force requests that the affected vendor establish a primary contact person who will continue to work with X-Force through the vulnerability disclosure process.

- Initial vendor notification begins when X-Force sends a draft advisory to the primary vendor contact.
  - X-Force will work closely with the affected vendor to reproduce the security vulnerability and will make reasonable effort to provide the vendor with information to assist in reproduction of the vulnerability. This includes detailed exploitation information, exploit code or proof of concept code, and any special testing instructions.
  - X-Force may also assist in testing vendor supplied patches or workarounds to confirm that the issue has been corrected. X-Force will incorporate the vendor's resolution or workaround into the Security Advisory whenever practical.
  - The vendor is notified that Internet Security Systems' customers who subscribe to the X-Force Threat Analysis Service (XFTAS) will be made aware of the existence of the vulnerability, as well as any countermeasures that are available, one business day after initial vendor notification. This process occurs during the Customer Notification Phase described later in this document.
- The vendor will have 30 days after initial notification to develop a fix unless other arrangements are in place. Procedural exceptions for accelerated disclosure are noted in Section V. of this document.
- X-Force contacts The MITRE Group (a not-for-profit research organization at http://www.mitre.org/) to obtain a Common Vulnerability and Exposures (CVE) candidate number (CAN) to establish a standard name for the security vulnerability.
- X-Force sends a final draft of the advisory to the vendor for review and comment before public disclosure.
- X-Force reserves the right to notify and/or coordinate with third-party organizations and/or governmental entities during the advisory release process.

III. Customer Disclosure Phase

- An X-Force Security Brief is made available to participating XFTAS customers one business day after the initial vendor notification.
- X-Force will revise each Security Brief document if more information becomes available during the ongoing advisory development process.

IV. Public Notification Phase

- Unless other disclosure arrangements have been made with the vendor in advance, X-Force will publicly disclose after 30 days from the initial vendor notification. X-Force will also disclose Security Brief to the ISS Alert Mailing List, FIRST, ISS Forum and Vuln-Watch. At the same time, a final X-Force Advisory document is published to the X-Force Web site (http://xforce.iss.net/alerts) and XFTAS.

V. Accelerated Disclosure/Procedural Exceptions

X-Force reserves the right to accelerate the publication of the vulnerability information at any time if one or more of the following events occur:

- The vendor issues a patch or announcement regarding the vulnerability.
- An in-depth discussion of the vulnerability appears on a public mailing list.
- Active exploitation of any form related to the vulnerability is observed on the Internet.

- ISS receives evidence from reliable sources that an exploit is available in the wild.
- The vulnerability is reported by the media.
- The vendor becomes unresponsive.

About Internet Security Systems (ISS)
Internet Security Systems (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical information assets from an ever-changing spectrum of threats and misuse. Software from Internet Security Systems dynamically detects, prevents and responds to sophisticated threats to networks, servers and desktops. Services include 24/7 system monitoring, emergency response and access to the X-Force, Internet Security Systems' renowned research and development team. Internet Security Systems is the trusted security provider for more than 10,000 corporate customers, including all of the Fortune 50, the top 10 largest U.S. securities firms, 10 of the world's largest telecommunications companies and major agencies and departments within U.S. local, state and federal governments. Headquartered in Atlanta, GA, 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 888-901-7477.