

December 2008



IBM Internet Security Systems™ X-Force®  
Research and Development Team  
Vulnerability Guidelines

---

Contents

---

- 2 Introduction
- 3 Guideline Terminology
- 4 The Vulnerability Disclosure Process

## Introduction

The IBM Internet Security Systems™ (ISS) X-Force® research and development team is a leader in the security industry in the areas of Internet threat research, discovery and remediation. The X-Force team is one of the oldest and best-known commercial security research groups in the world. This leading group of security experts researches vulnerabilities, exploit methods, malware, cybercrime, and many other issues that present a threat to organizations and individuals. The X-Force team develops assessment and protection technology for IBM ISS products and educates IBM customers and the public about emerging Internet threats.

Much of the X-Force team's efforts revolve around the discovery of new vulnerabilities in both hardware and software, and Internet threats that could potentially take advantage of these vulnerabilities. This research includes both active research of products and technologies and ongoing surveillance of Internet activity. When the X-Force team discovers a credible vulnerability, the details are released in an advisory, and protection and detection measures are delivered to IBM customers in Content Updates for IBM ISS products.

The following X-Force Disclosure Guidelines communicate the X-Force team's policies and procedures concerning the disclosure of vulnerability information to third-party vendors and the public. These guidelines seek to balance the protection needs of our customers with providing vendors a reasonable timeframe in which to respond to security issues.

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

## Guideline Terms

- X-Force Protection Advisories –Advisories contain information from original, X-Force team research. An advisory includes a synopsis of the security vulnerability or security issue, information regarding the impact of the discovered issue, a listing of affected versions, a detailed description of the issue, recommendations for managing and/or correcting the issue, IBM ISS product protection/detection for the issue, and other relevant/additional information.

The X-Force team releases all X-Force Protection Advisories on the IBM Web site at <http://xforce.iss.net/> for public viewing.

E-mail announcements for these advisories are sent to IBM Internet Securitysystems X-Force Threat Analysis Service (XFTAS) customers and to customers who have elected to receive IBM TrueBlue communications announcements.

- X-Force Protection Alerts –Alerts are released to provide additional information about an existing security issue and/or provide customers with information about IBM ISS product protection or detection for a security issue. The security information in Protection Alerts is released in accordance with the Disclosure Guidelines procedures. All X-Force Protection Alerts are released on the IBM Web site at <http://xforce.iss.net> for public viewing. Email announcements for these alerts are also made to XFTAS customers and to customers who have elected to receive IBM TrueBlue communications announcements.
- X-Force Threat Analysis Service –The X-Force Threat Analysis Service is a security intelligence service that delivers IBM customers customized information regarding the current state of Internet threats and the state of Internet security as a whole.

## The Vulnerability Disclosure Process

The X-Force team is actively involved in programs of original Internet and network security research. The disclosure of vulnerability information is a part of the research process and the results are provided to vendors as a public service and as such, are provided free of charge. Results and findings are also provided to IBM customers and to the public, but only after a prescribed period of time and only under a specific set of circumstances. These circumstances and the process surrounding the release of vulnerability findings are discussed below.

The X-Force team's vulnerability disclosure process is divided into four stages:

- I. Initial Discovery Phase
- II. Vendor Notification Phase
- III. Public Disclosure Phase
- IV. Accelerated Disclosure/Procedural Exceptions

### I. Initial Discovery Phase

X-Force team researchers discover and confirm a security vulnerability. The security vulnerability is documented in a draft X-Force Protection Advisory.

### II. Vendor Notification Phase

- A vendor is defined 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.
  - Initial communication is defined as any attempt to contact the vendor by e-mail and/or telephone either through established relationships or through publicly available contact information published within the vendor's Web site or sales collateral.
  - The X-Force team notifies the vendor of the vulnerability discovery and provides a timeline for private and public disclosure as outlined in this document. The X-Force team requests that the affected vendor establish a primary contact person who will continue to work through the vulnerability disclosure process.
- The X-Force team sends a draft advisory to the primary vendor contact.
  - The X-Force team will work closely with the affected vendor

to reproduce the security vulnerability and will make a 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.

- At their discretion, the X-Force team may also assist in testing vendor supplied patches or workarounds to confirm that the issue has been corrected. The X-Force team will incorporate the vendor's resolution or workaround into the Security Advisory whenever practical.
- The X-Force team assigns a MITRE corporation (a not-for-profit research organization at <http://www.mitre.org/>) Common Vulnerability and Exposures (CVE) number to establish a standard identifier for the security vulnerability.
- The X-Force team sends a final draft of the Protection Advisory to the vendor for review and comment.
- The X-Force team reserves the right to notify and/or coordinate with third-party organizations and/or governmental entities during the Protection Advisory release process.

### III. Public Notification Phase

The X-Force team will coordinate the public disclosure of the vulnerability in the X-Force Protection Advisory to coincide with the vendor's public disclosure.

### IV. Accelerated Disclosure/Procedural Exceptions

While every effort will be made to adhere to the disclosure process described in this policy, situations may arise that make adherence to these guidelines irresponsible in light of the danger presented to IBM customers and the general public, or simply unnecessary due to the affected vendor's own actions. In these instances, the X-Force team 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
- The X-Force team receives evidence from reliable sources that an exploit is in the wild
- The vulnerability is reported by the media
- The vendor becomes unresponsive

### For More Information

For answers to any questions concerning the details of the vulnerability disclosure process, or for more information on the X-Force team, or IBM Internet Security Systems, please contact use the contact form at: <https://www.iss.net/webForm.php?to=X-Force>



© Copyright IBM Corporation 2008

IBM Global Services Route 100 Somers, NY 10589 U.S.A.

Produced in the United States of America 08-07 All Rights Reserved

IBM, the IBM logo, Internet Security Systems, X-Force and Proventia are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.