MAY 2015

IBM Security
Research and Development Team
Coordinated Disclosure Guidelines

Introduction

The IBM X-Force® research and development team is a leader in the security industry in the areas of Internet threat research, discovery and remediation. Formed in 1996, the X-Force is one of the longest-lived and best-known commercial security research groups in the world. Today it includes not only vulnerability researchers, but also IBM Security AppScan Researchers, experts in identification and defense from web application threats, and IBM Security Trusteer Researchers, the leaders in threats focused on malware and financial fraud. This group of security experts research vulnerabilities, exploit methods, malware, and other issues that present a threat to an enterprise or an individuals computer systems. The IBM X-Force develops assessment and protection technologies for IBM Security solutions, generates threat intelligence data to provide customers with awareness of threats 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 threats such as network, endpoint and mobile application vulnerabilities, attack vectors, or malware, all of which could potentially put IBM customers at risk. This research includes both active research of products and technologies and ongoing surveillance of Internet activity.

The following Disclosure Guidelines communicate the IBM X-Force policies and procedures concerning the coordinated disclosure of a new threat to other parties. These guidelines seek to balance a broad protective response across multiple organizations and technologies through the coordinated disclosure of a threat, with open disclosure practices that strive to equip security professional with the information they require to protect the systems and organizations in their charge.

When the X-Force team discovers a credible threat, details may be initially disclosed privately to the vulnerable or targeted parties and after some period of time, may also be released publically in an X-Force Advisory and protection measures made available within IBM Security offerings as appropriate and practical.

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

Guideline Terminology

- **Threat** – The IBM X-Force defines a threat as a vulnerability in software or hardware, a new piece of malware or malware variant, attack vector, toolkit, or a tactic, technique, or procedure (TTP) on which the team provides guidance.
- **X-Force Advisory** – Advisories contain information from the IBM X-Force about the nature of a threat. X-Force advisories are available at this link: http://www.iss.net/threats/ThreatList.php

  - An advisory commonly includes many of the following pieces of information: (1) a synopsis of the security threat, (2) information regarding the impact to vulnerable and targeted parties, (3) a listing of affected versions and/or platforms, (4) a detailed description of the threat, (5) recommendations for mitigating and/or correcting the threat, (6) Details regarding which IBM offerings are able to provide protection or detection for the threat, and (7) other relevant or additional information as needed.
  - The IBM X-Force releases all X-Force Protection Advisories on the IBM web site (http://xforce.iss.net/threats/Threatlist.php) for public viewing. This information is also available via Twitter (@ibmxforce) and RSS feed (http://feeds.feedburner.com/xforcecriticalalerts)
  - E-mail announcements for these advisories are sent to IBM Security X-Force Threat Analysis Service (XFTAS) customers and to customers who have elected to receive IBM Security Connect communications announcements.

- **X-Force Threat Analysis Service** (XFTAS) – The X-Force Threat Analysis Service is a security service that provides IBM customers with customized information regarding the current state of Internet threats and the state of Internet security as a whole.
- **Traffic Light Protocol (TLP)** – The TLP designation describes how the recipient can utilize information it receives and furthermore how the recipient can share the information it has received. For more information refer to this URL: https://www.us-cert.gov/tlp.

The Disclosure Process

The IBM X-Force is actively involved in programs of original Internet, network and endpoint security research. The discovery of a new vulnerability, malware or TTP (tactic, technique or procedure) is a part of the research process and the results are disclosed to vendors or impacted parties as a public service and as such, are provided free of charge.

Research findings are also provided to IBM Security customers, and to the general public, but only after a coordinated disclosure process, or if no response, after a prescribed period of time, and only under a specific set of circumstances. These circumstances and the process surrounding the release of research findings are discussed below.

The X-Force team's threat disclosure process is divided into five stages:

i. Initial Discovery
ii. Private Disclosure
iii. Coordinated Disclosure
iv. Controlled Disclosure
v. Public Disclosure

i. Initial Discovery

IBM X-Force researchers discover, and confirm, new security threats in the form of a vulnerability (software or hardware), a new piece of malware, toolkit, or new tactics, techniques or procedures (TTPs), and will share that information with relevant parties *and* document that in an X-Force Advisory.

ii. Private Disclosure

IBM conducts private disclosure on two primary types of threats: vulnerabilities and malware. When IBM discovers a new vulnerability, it will contact the vulnerable vendor(s) to relay information about the discovery. This includes vulnerabilities or other threats targeting software, firmware, hardware or embedded system. In cases of multi-stakeholder events, such as vulnerabilities within open source libraries or malware attacking a given industry/sector, IBM will work with alliances (as discussed in section iii) in order to disclose and coordinate activities across multiple entities more effectively.

In the case of malware or other threat attacking one or more targeted entities, IBM will use a combination of IBM-internal communication channels to establish communication with the appropriate contact within the organization, or other established trust relationships in an attempt to identify the appropriate contact within the organization/entity to inform about the threat.

- 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.
- A target is defined as an organization or entity that may be generally or explicitly attacked by a given threat.
- 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. IBM will strive to use encrypted communications whenever possible.
    - The IBM X-Force requests that the affected vendor establish a primary contact person who will continue to work through the vulnerability disclosure process with IBM. To reduce the risk of disclosed information being misdirected, IBM will not send the threat details in the initial e-mail. The initial e-mail will be an introductory email used to identify the appropriate contact to provide the detailed technical information.
    - The IBM X-Force will notify the vendor of the threat discovery along with relevant information/data to replicate the issue and will provide a tentative timeline for a coordinated disclosure as outlined in this document. This includes detailed exploitation information; exploit code or proof-of-concept code, and any special testing instructions.
- The X-Force will provide a draft collateral after establishing contact with the vendor or organization.

  - Collateral is defined as any public facing content related to the research such as the X-Force Advisory, Blog post, or Whitepaper.
  - The X-Force 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.
  - At their discretion, the X-Force may also assist in testing vendor supplied patches or workarounds to confirm that the issue has been corrected. The X-Force will incorporate the vendor's resolution or workaround information / links into the Security Advisory whenever practical.
- The X-Force will assign a MITRE Corporation (a not-for-profit research organization; see http://www.mitre.org/) Common Vulnerability and Exposures (CVE) number to establish a standard identifier for the security vulnerability as well as the CVSS score.
- The X-Force reserves the right to notify and/or coordinate with third-party coordination organizations or ISAOs in order to enable a broader protective response, refer to section iii.

iii. Coordinated Disclosure

Depending upon the nature of the threat, the pervasiveness or type of entities impacted, IBM may provide early disclosure to other security vendors, intermediaries or entities under strict confidentiality in order to provide a more comprehensive protective response, and reduce the overall risk resulting from public disclosure. In this event, IBM will engage information sharing relationships to assist with the coordination and dissemination of information to impacted parties.

- Information sharing consortiums are defined as alliances or groups such as the ISACs, CERTs, ICASI or other known ISAO's (Information Sharing and Analysis Organizations) with which IBM has an established and trusted sharing relationship.
- Coordinated disclosures may occur when a threat is identified attacking multiple entities, when a vulnerability is identified in common code libraries (e.g., Open Source libraries), or other pervasive threats are identified requiring a coordinated response across multiple parties.

iv. Controlled Disclosure

The IBM X-Force may make certain protection information available to IBM customers in a controlled fashion prior to a public disclosure, depending upon the nature of the information and the ability of customers to act upon it. This information may be shared with IBM customers through various IBM services such as the X-Force Threat Analysis Service, IBM Managed Security Services (MSS) or IBM Accelerated Value Program (AVP).

v. Public Disclosure

The X-Force team will attempt to coordinate the public disclosure of the threat in the X-Force Advisory to coincide with the vulnerable vendor or entities public disclosure. IBM may also post relevant commentary in a blog or whitepaper regarding the given threat in an effort to provide further education on the nature of the threat. In some cases IBM may also choose to work with various press or media outlets to provide further education or awareness of a given threat.

- For vulnerabilities it is customary to expect vendors will make a patch available within **45 days**. However, we understand in some cases this is not reasonable given the nature of the issue, or potential dependencies that may necessitate a longer period of time to address. In these instances, IBM will work with the vendor to coordinate a suitable timeframe *normally no more than 90 days from initial disclosure unless circumstances warrant additional time.*
- Public disclosure of new malware variants, toolkits, tactics, techniques or procedures (TTPs) takes place once any explicitly attacked parties are notified and able to take protective measures. This is commonly **12-72 hours** prior to public disclosure.

Accelerated Disclosure and 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 unacceptable 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 instances of vulnerabilities, the X-Force team reserves the right to accelerate the publication of the vulnerability information in conjunction with communication with the vulnerable vendor at any time if one or more of the following events occur:

- The vendor releases a patch or issues an 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

In instances where malware is impacting an IBM customer the X-Force will make the best effort to identify and establish communication with the appropriate organizational contact. However, IBM reserves the right to accelerate the disclosure at any time if one or more of the following events occur:

- Another research organization discloses information on the threat

- There is discussion within the various research networks about the malware variant
- Disclosure of the vulnerability is necessary to stem off further infections or impacted

In the event of an accelerated response, IBM will communicate to the affected parties using the last successful communication mechanism of the change in timeline.

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 Security, please contact us.