SOLUTIONARY®
AN NTT GROUP SECURITY COMPANY

Solutionary Vulnerability Disclosure Program (SVDP)

presented by

Security Engineering Research Team (SERT)

Table of Contents

Solutionary Vulnerability Disclosure Program

The goal of the Solutionary Vulnerability Disclosure Program (SVDP) is to distribute vulnerability information to the public in a controlled manner, following common industry practices associated with disclosing newly identified vulnerabilities. The vulnerabilities disclosed during this process have been identified by the Solutionary Engineering and Research Team (SERT). It is not the intention of Solutionary to release vulnerability information before first attempting to contact the software or hardware vendor and discussing patch and remediation options.

Solutionary Vulnerability Disclosure Lifecycle

In lieu of pre-existing contractual arrangements, Solutionary follows a three step process for the Solutionary Vulnerability Disclosure Lifecycle (SVDL), as described below.

Step 1 - Vulnerability Discovery

During routine vulnerability research activities, it is possible that research being performed may result in the discovery of a vulnerability not previously disclosed publicly. Upon discovery of a new vulnerability, Solutionary will verify, using various open-source vulnerability databases, that the vulnerability has not been previously discovered or disclosed.

Vulnerability databases referenced for verification include but are not limited to the following resources:

- Secunia: http://secunia.com/advisories/
- SecurityFocus: http://www.securityfocus.com/bid
- Open Source Vulnerability Database (OSVDB): http://osvdb.org/
- CVE: http://cve.mitre.org/cve/
- ExploitDB: http://www.exploit-db.com/

Should Solutionary determine that the discovered vulnerability has not been previously discovered or disclosed, Solutionary will advance to step 2 of the SVDL process.

Step 2 - Vendor Notification

The SERT will attempt to contact the vendor via e-mail and notify them of the newly discovered vulnerability. As part of the process, Solutionary sends e-mails to multiple e-mail notification addresses at the vendor's primary e-mail domain. Unless a specific e-mail address is provided for vulnerability disclosures or security-related issues on the vendor's Web site, Solutionary sends the initial notification to the following e-mail aliases: security@, info@, sales@, support@, and security-alert@.

During this initial e-mail notification, Solutionary will indicate the plan to disclose the vulnerability according to a specific timeline. The vendor is encouraged to reply to the initial e-mail and work with Solutionary to determine a solution timeline. The timeline for release and notification is outlined in step 3. The initial e-mail will also provide the vendor with information about the vulnerability, scope of vulnerability, disclosure timeline, and other useful information for reproducing the issues discovered. In cases where proof-of-concept (POC) exploit code is available, Solutionary will provide and securely transmit such information upon request to the vendor. This includes all code and information required to allow the vendor to verify the vulnerability and develop an appropriate solution.

Simultaneous with the vendor being notified, Solutionary may implement vulnerability detection and protection for its customers through the ActiveGuard® managed security service.

If the SERT does not receive acknowledgement of the vulnerability or indication the e-mail was received and reviewed by the vendor, the SERT will send a follow-up notification e-mail 15 calendar days after the initial notification e-mail. Additionally, the SERT will attempt to contact the vendor via telephone if appropriate contact information is available.

Should there be a lack of response from the vendor; Solutionary will still maintain the predetermined release schedule. All vulnerability releases follow the timeline as indicated to the vendor through this policy where possible.

Step 3 - Public Notification

Public notification and disclosure of the vulnerabilities discovered and reported to the vendor is an important part of the SVDL. Solutionary will publicly disclose the vulnerability information approximately 45 calendar days from the date Solutionary sends the initial notification of intent to release to the vendor.

Public disclosure will include the release of the vulnerability details on the Solutionary Web site (http://www.solutionary.com). Solutionary will also release the vulnerability details through industry standard vulnerability database Web sites.

Regardless of vendor acceptance or validation of the vulnerability, the SERT will release the vulnerability to the public upon completion of the steps defined above. Unless there are exceptional circumstances where the SERT has determined a delayed public release period is warranted; Solutionary will follow the previously described disclosure process. All decisions regarding final public release status are made at the discretion of the SERT.

Early Disclosure Guidelines

In certain cases it may become necessary to release the vulnerability details prior to the initial release schedule. Some of these cases may include but are not limited to the following:

- Vendor releases a patch and acknowledges the vulnerability publicly in advance of the indicated timeline
- Wide-spread exploitation of the vulnerability is evident
- Media coverage about the vulnerability exposes the vulnerability to the public

Solutionary Vulnerability Disclosure Program Change Control

Solutionary updates the SVDP policies, processes, and procedures on a regular basis. Solutionary reserves the right to modify the policies and procedures associated with the program without notice to vendor. Vendors are encouraged to contact Solutionary should clarification of the disclosure policy be required.

For specific questions about the SDVL process, please send inquires to the following e-mails: vulnerabilityresearch@solutionary.com or sert@solutionary.com.

About Solutionary

Solutionary, an NTT Group security company (NYSE: NTT), is the next generation managed security service provider (MSSP), focused on delivering managed security services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

For more information, visit www.solutionary.com

Contact Solutionary at SCSManagement@solutionary.com or 866-333-2133

Solutionary, an NTT Group security company, is the next generation managed security services provider (MSSP), focused on delivering managed security services and global threat intelligence.

SOLUTIONARY

Solutionary.com

Solutionary, Inc.

9420 Underwood Avenue

Omaha, NE 68114

2020SR 05/14