XIPITER

VULNERABILITY DISCLOSURE POLICY

Xipiter LLC
New York, NY 10128
1.855.XIP.ITER
(1.855.947.4837)
info@xipiter.com

Friday, September 6, 2013

Introduction

Responsible Disclosure is an often debated subject within Information Security circles. The purpose of this document is to define "Responsible Disclosure" as it is understood by Xipiter and to offer transparency with regard to Xipiter's process for vulnerability disclosure, vendor notification, and eventual public disclosure of vulnerabilities. This document defines terms and sets clear expectations through the following sections of this document:

- **Introduction:** This section.
- **Disclosure Process Details** Summary of the project and the work to be perform as understood by Xipiter. This section also summarizes TPVision obligations ,technology requirements, and other project prerequisites to be fulfilled and supplied by TPVision Inc.
- **Notification Templates** Summary of the work product resulting from the Services performed.
- **Disclosure Template:** Price or time and materials rates, payment and special terms, and contact information. Also includes signatures section authorizing the work described in this document.
- **Disclosure Flowchart:** A bit about who you will be working with on this project.

STATEMENT OF INTENT:

Xipiter's Responsible Disclosure Policy is designed to offer software and hardware manufacturers education, assistance and coordination regarding identified security issues, as well as provide end users with a timely and desirable resolution. This policy sets forth Xipiter's intentions and guidelines for communication between Xipiter and manufacturers so that we can better work together.

SCOPE

This policy covers all vulnerabilities that Xipiter discovers and intends to disclose publicly.

AUDIENCE

This policy is intended for vendors of affected software and hardware and clients of Xipiter. To ensure transparency, this document is available to the public and is accessible from Xipiter's website at the following location:

http://www.xipiter.com/research

SUMMARY

Should a vulnerability be discovered internally at Xipiter, Xipiter will notify the product vendor. The notification will contain details of the issue as well as next steps for resolution and coordinated public disclosure. Any next steps will specify timing that is assumed to be agreed upon in the absence of acknowledgement by the vendor within a reasonable timeframe, as further defined in the process details section of this policy.

DISCLAIMER

This policy is made available solely for informational purposes and in accordance with Xipiter's understanding of information currently available to Xipiter. Legal and business developments are prone to change, and may not be entirely reflected herein. Xipiter does not represent, warrant or guarantee that this policy is complete, accurate or up-to-date, nor does Xipiter offer any certification or guarantee with respect to this disclosure policy. The information provided is AS IS, and Xipiter assumes no responsibility for errors, omissions or damages resulting from the use of or reliance on the information herein or disclosed by Xipiter. Prior to acting pursuant to this policy or relying on any information herein, readers should obtain professional advice and seek to understand all facts and circumstances related thereto.

CONTACT:

Xipiter legal counsel can be reached at:

1.855.XIP.ITER (int'l) 1.646.783.3999

or

legal@xipiter.com

All general contact with Xipiter or Xipiter staff can be done at:

1.855.XIP.ITER

Fax: 1.917.746.9832

info@xipiter.com

Disclosure Process

Xipiter's Responsible Disclosure process consists of the following three phases.

1. Vendor Notification
2. Vendor Coordination
3. Public Disclosure

The Vendor Notification phase includes Xipiter' initial communications with the product vendor. During the Vendor Coordination phase, Xipiter and the vendor coordinate timelines and details of issues that arise in the planning and development of the solution. Finally, during the Public Disclosure phase, details of the issue and related solution are published.

PHASE 1: VENDOR NOTIFICATION:

Xipiter will verify and document each vulnerability prior to Vendor Notification. Vendor Notification is the first phase of the public disclosure process, where Xipiter' goal is to provide vulnerability details necessary for the vendor to begin its internal resolution process.

Appendix A contains a template used in crafting the Vendor Notification. Appendix B includes a template used in the initial draft of the Public Disclosure and is intended to be included in the Vendor Notification.

If the vendor has not acknowledged receipt within 30 business days of the original notification, Xipiter will retransmit the vulnerability details to the original contact and at least one secondary contact, if a secondary contact is publicly available. If the vendor allows an additional ten business days to elapse following the second notification (40 business days since original notification) without acknowledging the information, vulnerability details will be re-sent not only to the previous two contacts, but also to Xipiter's customers or other stakeholders at Xipiter' discretion.

If the product vendor does not respond to any of the three notification attempts within an additional ten days following the third notification (50 business days since original notification), or if the vendor indicates that it does not wish to coordinate disclosure, Xipiter may elect to issue a public advisory (see Public Disclosure).

Acknowledgement of the notification by the vendor should include all of the following items:

- Vendor confirms the vulnerability information is received and the schedule for investigation.
- Vendor provides a point of contact responsible for coordinating and tracking information on the issue from within its organization.
- Vendor provides an estimate as to when it expects to complete its initial investigation of the security issue provided in the notification.

Once the vendor has successfully acknowledged the notification and responds accordingly, the disclosure process continues to the Vendor Coordination phase.

PHASE 2: VENDOR COORDINATION:

Upon successful acknowledgement of the notification, Xipiter will work with the vendor to determine how the security issue will be addressed. The following tasks are included within this phase:

- At the vendor's request, Xipiter will provide additional information to assist in the development of a solution.
- At the vendor's request, Xipiter will review proposed solutions for effectiveness in at least one version of the product.
- At the vendor's request, Xipiter will review proposed solutions for effectiveness in at least one version of the product.
- The vendor and Xipiter will exchange proposed timing for public disclosure of the issue and related solution for mutual approval.

If vendor responses to all communications in this phase are not received within five business days, Xipiter may move directly to the Public Disclosure phase.

Furthermore, during the Vendor Coordination phase it is common for vendors to request a proof-of-concept (PoC) to trigger the vulnerable code. Xipiter believes PoCs are useful tools in a vendor's remediation efforts, especially when developers of the affected code are no longer available. Xipiter may, at its discretion, satisfy vendor requests for PoCs. Additionally, Xipiter may release the PoCs to the public after the Public Disclosure phase completes and a solution has been made available.

Requests by vendors for production grade exploits are sometimes made when the vulnerability's proposed criticality is doubted. Given that this type of request implies that the organization that authored the software is uncertain of the vulnerability's criticality, it follows that users and administrators who have less working knowledge of the product have an even higher level of uncertainty. Therefore, Xipiter may, at its discretion, deliver the exploit to the vendor upon request; however, exploits of a similar quality may also be furnished to the public in an effort to supply end users with the information necessary to make an informed decision regarding their security posture.

PUBLIC DISCLOSURE:

Public Disclosure is the final phase of the disclosure process. During this phase, Xipiter' intent is to provide information on the vulnerability and related solutions. Public Disclosure may be initiated either by completing the Vendor Coordination phase or through a process failure in prior phases.

During the Public Disclosure phase Xipiter, and optimally the vendor, will disseminate information on the vulnerability and related solution to the public. Xipiter may disseminate information through public e-mail lists, web pages or any other medium it deems appropriate to reach the intended audiences.

Public Disclosure information is intended to be used by the following groups:

- Protectors, which include security vendors and administrators, may use the information to develop technologies or solutions to assist in defending or alerting the public on attacks exploiting the related vulnerability.
- Product users and owners may use the information to prioritize remediation resources.
- Consultants may use the information during engagements to identify the presence of known issues in a client's environment and provide accurate details of the respective impact.

The level of detail that is included in the Public Disclosure to each of the above stakeholder groups will vary.

EXCEPTIONS:

Xipiter reserves the right to vary the terms of its Responsible Disclosure Policy in light of possible adverse consequences to clients and the public, information that is already public, or the vendor's response.

GENERAL NOTES:

Xipiter uses the following email address for all disclosure communications:

research@xipiter.com

Appendix C contains the public key that can be used in association with the above address.

Email is used as the default communication method, unless a vendor has published preferences for vulnerability disclosure communications. When a vendor has published alternate preferences, it is at Xipiter' discretion whether or not to honor the published preference.

All vendor communications will be directed to the vendor's publicly identified security contact, if one is made available to the public via the vendor's primary website. If a security contact cannot be identified or becomes unresponsive, Xipiter will identify and use a contact from the vendor's product support team to the extent such a contact is known or can be publicly identified.

All public communications will be directed to mailing lists and posted to Xipiter's public site, or any others deemed appropriate. Records of all communications will be maintained indefinitely, but at a minimum until a solution to the vulnerability is available.

Appendix A: Notification Template

Date: [Today's Date]
To: [Recipients]
From: Xipiter Research<research@xipiter.com>
Subject: Notification of Security Issues in [Product(s)] [Issue Id]

This message serves to notify appropriate personnel of security issues related to [Company] products. Please forward this message to the appropriate party if it is not you. Enclosed you will find details concerning a security issue in one or more of your products. We believe malicious users could exploit this issue to compromise the security of your customers. Xipiter follows its Responsible Disclosure Policy, which can be found at the following location:

http://www.xipiter.com/research/

As defined in our policy, we would like to offer assistance in the resolution of this issue and coordinate any disclosure of it.

Once you have reviewed the enclosed material and our disclosure policy, please respond with an acknowledgement for this notification within 30 business days to indicate your intent of participation in a coordinated effort on this issue.

For tracking purposes, please retain the subject line in all correspondence related to this issue.

We look forward to working with you.

-- Xipiter

Appendix B: Disclosure Template

vulnerability summary

→ The tables below are categorical lists overviewing of all of the issues discovered during the project. It is to be used by both the Xipiter and AcmeTron to ensure that all vulnerabilities are being successfully managed. Most of the tables are self-documenting, however the definitions of the status columns are described below. ¶

¶

STATUS DEFINITIONS ¶

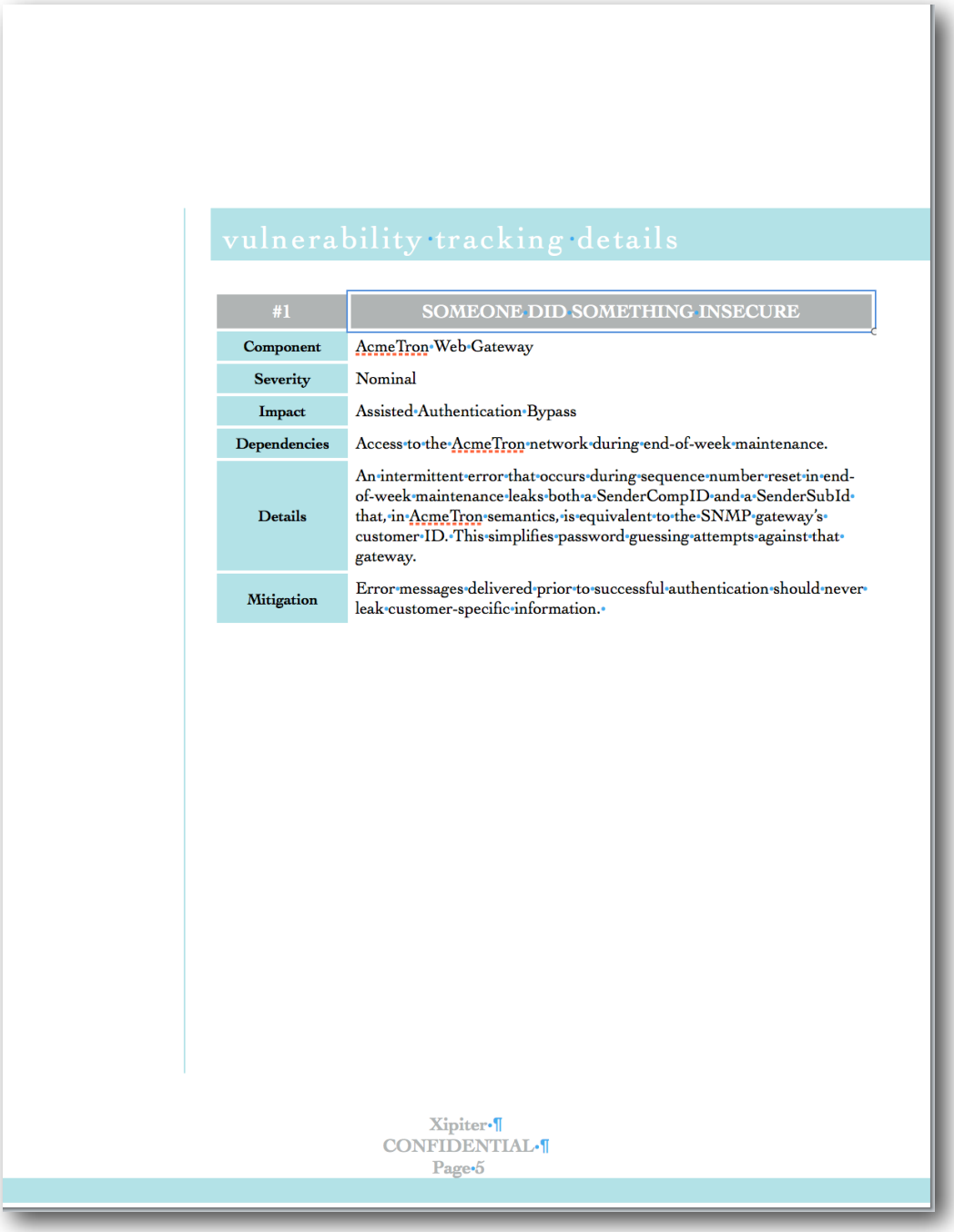
- Reported: Xipiter has found what we believe to be a vulnerability. At the time of this version of this document, Acmetron is yet unaware of this vulnerability. ¶
- Unreported: Xipiter has found what we believe to be a vulnerability. At the time of this version of this document, Acmetron is yet unaware of this vulnerability. This document thus represents the first time that the vulnerability is being formally communicated to Acmetron. ¶
- Confirmed: Acmetron confirmed the existence of the vulnerability and consensus on the risk has been reached. ¶
- False Positive: The vulnerability discovered by Xipiter is mitigated or does not exist. ¶
- Regression: The vulnerability has been fixed by Acmetron and requires validation from Xipiter. ¶
- Resolved: Both parties (Xipiter and Acmetron) agree that the vulnerability has been fixed and/or mitigated. ¶

VULNERABILITY CHART ¶

#	ISSUE	SEVERITY	STATUS
1	Someone did something insecure	High	Resolved
2	There was additional functionality left in	Low	Reported
3	Someone messed up something and it is broke	Low	*Unreported*
4	The broken thing above made something broke	Low	Reported
5	Insecure use of otherwise secure technique	Medium	Resolved

Xipiter ¶
CONFIDENTIAL ¶
Page 4

Appendix B: Disclosure Template continued



vulnerability tracking details

#1	SOMEONE DID SOMETHING INSECURE
Component	AcmeTron Web Gateway
Severity	Nominal
Impact	Assisted Authentication Bypass
Dependencies	Access to the AcmeTron network during end-of-week maintenance.
Details	An intermittent error that occurs during sequence number reset in end-of-week maintenance leaks both a SenderCompID and a SenderSubId that, in AcmeTron semantics, is equivalent to the SNMP gateway's customer ID. This simplifies password guessing attempts against that gateway.
Mitigation	Error messages delivered prior to successful authentication should never leak customer-specific information.

Xipiter ¶
CONFIDENTIAL ¶
Page 5

Appendix C: PGP Key Fingerprint

PGP Key is 4096 so too long to paste. Instead here is the fingerprint:

9880 C46E BB92 3692 2034 399D 8528 1F4E 16E8 F0E8