BROCADE
A Broadcom Inc. Company

Brocade Security Vulnerability Management

Responsible Disclosure Policy

Version 9.0;

August 2019

Introduction

Brocade Communications Systems (Brocade) is committed to resolving vulnerabilities to meet the needs of its customers and the broader technology community. This document describes Brocade policy for receiving reports related to potential security vulnerabilities in its products and services and the Company's standard practice with regards to informing customers of verified vulnerabilities.

Brocade Product Security Incident Response Team (Brocade PSIRT) is a global team that manages the receipt, investigation and internal coordination of security vulnerability information related to Brocade Fibre Channel technology products from Broadcom. This team coordinates within Brocade the investigation, and if needed, identify the appropriate response plan. Brocade PSIRT doesn't deal with technical assistance problems.

Customers of Brocade should continue to report product related defects, including general security concerns and configuration assistance issues, to Brocade Global Support. The Brocade Global Support can also help with software upgrades for security updates.

Reporting a Vulnerability to Brocade.

Brocade welcomes reports from Reporters: security researchers, individuals, coordinators, industry groups, government organizations, vendors and other sources about potential vulnerabilities in Brocade Fibre Channel technology products from Broadcom. Brocade PSIRT can be contacted by Email at brocade.sirt (at) broadcom.com.

Brocade encourages reporters to use the template to facilitate the collection of key information about the vulnerability (See Appendix A). Brocade also encourages the encryption of sensitive information that is sent in email messages. The Brocade PSIRT supports encrypted messages via PGP/GNU Privacy Guard (GPG). The Brocade PSIRT public PGP Key is available on multiple public key servers.

Brocade Product Security Incident Response Team Process.

The steps below outline the lifecycle of a reported security Incident to Brocade PSIRT.

Receipt Vulnerability.

When Brocade PSIRT receives a report of a potential vulnerability from a third party, Brocade PSIRT acknowledges receipt of the report, logs the issue with the supporting details and notifies the appropriate product teams as to the existence of the potential vulnerability for analysis.

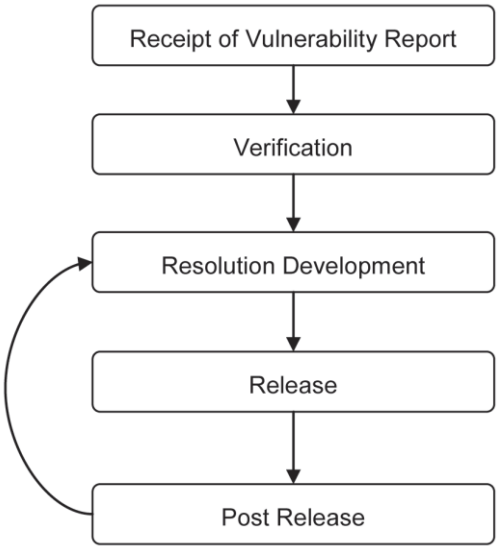

FIG.1. Vulnerability report lifecycle.

Verification/Triage/Prioritization.

Brocade PSIRT and Products Team investigate the report; try reproducing the environment and behavior reported by the Reporter. This may be a preliminary investigation, focused primarily on the need for further effort. The investigation determines whether the report constitutes a vulnerability or not. Brocade PSIRT uses the version 3.1 of the Common Vulnerability Scoring System (CVSS) https://www.first.org/cvss/ and other factors such as the risk impact statement, the availability of a publicly available exploit, in assigning an internal priority to the issue.

After the initial analysis, the vulnerability undergoes further investigation by the product team to determine the underlying cause and possible methods of exploitation. The team completes the remediation plan for the vulnerability, taking into consideration the affected versions. In some cases, Brocade PSIRT may request additional information from the Reporter to understand the environment in which the vulnerability appears the code version, ways to reproduce the issue, potential exploitation methods, etc.
Brocade PSIRT may communicate with the Reporter the result at the end of the investigation. If Brocade does not consider the reported issue as a valid vulnerability, the Reporter is also updated. If the Reporter disagrees with the conclusion, Brocade PSIRT will make every effort to address the concerns.

The Brocade PSIRT manages all sensitive information on a highly confidential basis and distributes information internally only to the Product Teams and individuals who have a legitimate need to know and can actively assist in the resolution.
Similarly, the Brocade PSIRT asks incident reporters to maintain strict confidentiality until complete resolutions are available for customers and have been published by Brocade PSIRT on Brocade Security Advisory website https://www.broadcom.com/support/fibre-channel-networking/security-advisories through the appropriate coordinated disclosure. With the agreement of the Reporter, the Brocade PSIRT may acknowledge the Reporter's contribution during the public disclosure of the vulnerability.

Resolution development phase.

Brocade develops a resolution plan for vulnerabilities reported. Resolution development may involve more detailed investigation of the root cause of the vulnerabilities and determination of code branches and other products affected by the same or similar vulnerabilities. Brocade also researches if there are workaround applicable. Brocade typically develops remediation and mitigation techniques and performs positive tests to determine that the remediation works correctly and negative (regression) tests to provide assurance that the remediation does not disrupt existing functionalities. Brocade may develop emergency patches for high priority issues. Brocade will keep the Reporter informed of the expected schedule for fixes and the security advisories.

Release phase.

Once the remediation is available, Brocade provides the remediation and mitigation information to Customers, typically in the form of vulnerability advisory and software patches or updates. The advisory explains the issue, how it affects Brocade products. The advisory also provides steps for mitigation including workarounds and how to apply them. In specific circumstances, Brocade may release an advisory before a remediation is available, particularly in cases of active exploitation or public discussion.

Brocade publicly disclosed vulnerabilities include details such as the Common Vulnerability Scoring System (CVSS) Base score and vector, a reference to the assigned Common Vulnerabilities and Exposures (CVE) identifier, remediation for the affected offering(s) and other relevant links that may cover additional information.

Post-release phase

Brocade collects feedback from Reporters, Users and updates remediation and mitigation information as necessary.

Brocade PSIRT recommends contacting Brocade's Global Support for instructions on installing these software updates, patches and for problems or questions. All aspects of this process are subject to change without notice and on a case-by-case basis. No particular level of response is guaranteed for any specific issue or class of issues.

Publication.

Brocade Security Advisory.

Brocade Security advisories are posted after a window time at Brocade's discretion to allow customers and partners to apply required patches. The advisories are made public at the following webpage:

https://www.broadcom.com/support/fibre-channel-networking/security-advisories

CVE Reporting.

For newly found vulnerabilities affecting a Brocade Fibre Channel San product, Brocade assigns CVE IDs and publicly discloses in CVE database.

Working with Reporters

Brocade is grateful to Reporters identifying vulnerabilities and working with us to ensure the safety of Brocade Customers. Brocade kindly asks Reporters to not share or publicize an unresolved vulnerability with/to third parties. By following this Responsible Security Disclosure Policy, Brocade PSIRT and associated development organizations will use reasonable efforts to:

- Respond quickly and acknowledge receipt of the vulnerability report
- Provide an estimated time frame for addressing the vulnerability report
- Notify Reporters when the vulnerability has been fixed
- Notify Reporters when the fix will take time due to the complexity of testing required

Brocade agrees to not take legal actions claims against Reporters related to disclosures submitted to Brocade PSIRT providing the following:

- Reporters don't compromise the privacy or safety of our customers and the operation of Brocade products and services.
- Reporters don't cause harm to Brocade, customers, or others.
- Reporters don't violate any criminal law.
- Reporters don't publicly disclose vulnerability details before Brocade confirms completed remediation of the vulnerability

Appendix A: Vulnerability Report Template.

a. Researcher Contact information

- Public PGP key
- Do you want to be credited?
- How do you want to be credited?

Note: If we publish a document based on this report, we will credit you unless otherwise specified.

Do you want us to acknowledge you by name in any published document about this vulnerability?

b. Vulnerability Description

- What Software, Systems are affected

(Name, Version numbers, Platforms and Configuration)

- Description of the vulnerability

Technical detail, proof of concept and steps to reproduce

- What is the vulnerability?

Provide sufficient technical detail

- How does an attacker exploit this vulnerability?
- Steps to reproduce
- What does an attacker gain by exploiting this vulnerability?

(i.e., what is the impact?):

- How was the vulnerability discovered?

(Tools and techniques used)

- Is this vulnerability publicly known?
- Is there evidence that this vulnerability is being actively exploited?
- Do you plan to publicly disclose this vulnerability yourself?

Revision History

Version 6.0: December, 2018

Minor wording changes

Version 7.0: February, 2019

Minor Wording changes.

Version 8.0: June, 2019

Minor Wording changes. Information about Brocade Global Support.

Version 9.0: August, 2019

Update to reflect the use of Common Vulnerability Scoring System Version 3.1