nccgroup

Global Vulnerability Disclosure Policy

Global Vulnerability Disclosure Policy

Issue date: 2 April 2025
Version: 1.0

What is this?
NCC Group's global policy for the disclosure of vulnerability information

Who does it apply to?
This policy applies to all colleagues who wish to disclose vulnerability information outside of NCC Group

What are the key points?

- NCC Group adheres to industry agreed responsible disclosure guidelines to ensure vendors have all the information they need to fix security bugs
- The ultimate goal of vulnerability disclosure is to help build a more secure and resilient future

What action should I take?

- Read the policy to understand how it applies in the context of your role
- Refer to the policy when planning to disclose any vulnerability information
- Contact the Global Research Director if any uncertainty remains regarding vulnerability disclosure

Global Vulnerability Disclosure Policy
Issue date: 2 April 2025
Version: 1.0

Contents

1. Introduction

NCC Group believes that security research is performed to keep users of technology safe from its weaknesses and informed of the risks they are taking through its use. Therefore, when NCC Group discovers flaws in software, we attempt to responsibly disclose relevant information to the public in a way that minimises the harm of the flaw and encourages further critical analysis of systems and security.

This policy explains the general structure of how NCC Group conducts the process of responsible vulnerability disclosure to our clients, software vendors, organisations tasked with critical infrastructure protection and the Internet public.

The aim of this policy is to enable all parties to understand and address vulnerabilities expeditiously in their environment and to minimise the risks that vulnerability information poses.

Technical Advisory – Technical Advisories contain technical information from original, internal research. This advisory type will contain:

- A management overview of the security vulnerability
- Information regarding the impact level of the issue
- A timeline of bug discovery and mitigation
- A list of affected product versions
- A technical description that can be used to validate and replicate the issue
- Recommendations for correcting or mitigating the issue
- Any other relevant vulnerability tracking information

2. Vulnerability Disclosure Goals

The goals of this policy are as follows:

- To specify the manner in which NCC Group discloses vulnerability information
- To inform software vendors of our policy regarding disclosure
- To inform the wider Internet community of NCC Group's policy
- To provide a rationale for our policy, in the hope that other organisations and individuals adopt a responsible disclosure policy

3. Vulnerability Disclosure Process

The disclosure of vulnerability information is provided as a public service to vendors, our clients and the general Internet population. The vulnerability disclosure process is divided into five logical stages:

1. Initial Discovery
2. Vendor Notification
3. Client Mitigation
4. Public Disclosure (Technical Advisory)
5. Accelerated Disclosure (in exceptional circumstances)

Following the initial discovery of a security vulnerability, NCC Group will follow the steps described below:

3.1 Initial Discovery Phase

When a vulnerability is discovered, the team will investigate the potential impact of the vulnerability. This includes identifying whether the vulnerability is exploitable, is limited to denial of service (DoS) attacks, diverges from security best practices, or otherwise constitutes a security flaw.

If a vulnerability is discovered during a paid engagement, NCC Group works closely with the client to find a solution. NCC Group may elect to notify relevant third party software and systems vendors of the existence of critical vulnerabilities discovered during security testing engagements, however NCC Group will only make such a notification where it reasonably considers that the existence of the vulnerability should be brought to the relevant vendor's attention to prevent harm to other users of the software or systems, and that NCC Group making the notification is generally in the public interest. NCC Group will limit the content of any notification to the existence of the vulnerability in question, and will not provide any data or information specific to the client or which might reasonably be expected to identify the client.

At the conclusion of this stage, a draft Technical Advisory document is produced and submitted for approval by the Global Research Leads

Where appropriate, this information can then be added to detection logic within NCC systems to help identify if the vulnerability is being exploited in the wild.

3.2 Vendor Notification Phase

During this phase, the vendor is officially notified of the vulnerability and a communication channel is established. The initial draft Technical Advisory is passed to the vendor for detailed discussion. NCC Group will provide reasonable assistance to the vendor in understanding the significance of the discovered vulnerability. If the vendor utilises a Bug Bounty programme for vulnerability disclosure then this mechanism can potentially be used by colleagues at this stage of the process.

The stages to this vendor notification phase are as follows:

1. NCC Group makes a reasonable effort to establish communication with the affected vendor(s)

NCC Group defines a vendor as any company, group, or organisation that develops and provides software, hardware, or firmware applications, either for sale or as part of a free distribution. NCC Group defines initial communication as any attempt to contact the vendor via an approved email address or telephone number, or by sending an e-mail to security@, security-alert@, support@, info@, and secure@ vendor - with information that a vulnerability has been discovered. However, no sensitive vulnerability details are sent until a secure communications channel has been established. Vendor contacts are identified through pre-established relationships and/or through publicly available contact information published within the vendor's web site or sales material.

A successful conclusion to the initial communication is the establishment of an agreed communication channel and the vendor establishing a primary contact person who will continue to work with NCC Group through the vulnerability disclosure process.

NCC Group prefers to use encrypted email as the communication channel for vulnerability information.

2. NCC Group formally notifies the vendor of the discovery of the vulnerability and will distribute information on the schedule outlined in this document

Initial vendor notification begins when NCC Group sends through a draft of the Technical Advisory to the primary vendor contact and also a link to this policy document on the NCC Group website.

At this point NCC Group will clearly inform the vendor of our intent to publish the information and the schedule for such publication. This is generally 90 days after either successful initial communication with the vendor or after all reasonable attempts to communicate with the vendor have failed to elicit a response. If a fix for the issue is made available to users before the end of the 90-day deadline, the Technical Advisory will become public 30 days after the fix was made available. Otherwise, the Technical Advisory will become public at the deadline.

NCC Group will make reasonable effort to provide the vendor with information to assist in the reproduction of the vulnerability. This may include detailed exploitation information, proof of concept code and any special testing instructions that may be required. NCC Group may also assist in testing vendor-supplied patches or workarounds to confirm that the issue has been corrected. This could include liaising with an NCC Group client through which the vulnerability may have originally been discovered. NCC Group will look for regular updates as to the status of the vulnerability during this phase.

As part of any Secure Development Lifecycle process NCC Group would recommend to vendors that further checks are performed to ensure that this type of issue is not systemic within their code base.

NCC Group will incorporate the vendor's resolution or workaround into the Public Vulnerability Statement document where possible.

3. The vendor is unresponsive, will not fix the issue or does not consider it a security risk

If the vendor could not be contacted, becomes unresponsive, decides not to fix the reported issue or does not consider the reported issue to be a security risk, NCC Group may begin an Accelerated Disclosure process (section 3.5 below).

4. The issue is a fundamental design flaw

If the reported issue relates to a design flaw which will require significant changes to the product to fix, but can be mitigated with a workaround, NCC Group may begin an Accelerated Disclosure process (section 3.5 below).

3.3 Client Mitigation Phase

NCC Group is committed to ensuring that our clients receive the best and most timely security advice available. Consequently, after discovering a vulnerability, NCC Group will liaise with our clients to ensure that they are adequately protected against the vulnerabilities in question.

3.4 Public Disclosure Phase

NCC Group believe that discussion of exploit techniques and countermeasures is essential in order to promote more accurate assessment of risk and to provide more effective general solutions to security problems. At the point of public disclosure, NCC Group may release tools that aid in the vulnerability's discovery and confirmation of its exploitability on affected systems.

If a new or unusual technique is required to exploit an issue, and we do not believe the technique has been discussed in the public domain before, we may release technical examples discussing the technique, its implications and any relevant countermeasures. These examples will not include

functional exploit code, and wherever possible they will be minimal code examples that illustrate the technique.

NCC Group may decide that in certain circumstances public disclosure of a Technical Advisory is inappropriate - this will be decided on a case-by-case basis.

3.5 Accelerated Disclosure / Procedural Exceptions

NCC Group reserves the right to accelerate the publication of the vulnerability information at any time. For example, disclosure might be accelerated if one or more of the following events occur:

- 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
- NCC Group receives evidence from reliable sources that an exploit is available in the wild
- The vulnerability is reported by the media
- Despite reasonable efforts, an appropriate contact within the vendor organisation cannot be identified
- The vendor becomes unresponsive

3.6 Issue discoverer leaves NCC Group during this disclosure process

Occasionally the original discoverer of an issue may leave NCC Group to work for another company during this disclosure process. When this occurs the discoverer will still be credited on the Technical Advisory, however it is their responsibility to hand over the details of all communications that have occurred with the vendor during the disclosure process to appropriate research management staff prior to their departure so that the disclosure process can be successfully completed.

4. Exceptions to Disclosure Guidelines

Potentially unwanted software and/or hostile software are exempt from the disclosure process. This includes spyware, adware, viruses, worms, rootkits, monitoring software and any other software that acts against users' interests. Any research into this class of software is eligible for disclosure without notifying the creators/maintainers. NCC Group may classify any piece of software in this category at its own discretion but typical examples include software that:

- Installs without consent
- Doesn't provide an uninstall mechanism
- Spreads virally
- Hides its files/processes or any other resource