

NGS Software Vulnerability Disclosure Policy

Introduction

Next Generation Security Software Limited (NGS) is the recognised world leader in the discovery of new security vulnerabilities. The NGS Insight Security Research team (“NISR”) is dedicated to discovering vulnerabilities and design weaknesses that potentially expose operating systems, applications and appliances to attack or misuse. This discovery process includes the active research of products and technologies and detailed analysis of security flaws discovered during NGS Consulting security assessment engagements. Where appropriate, these security discoveries are released in the form of advisories and delivered within product updates to NGS Software’s commercial suite of advanced vulnerability assessment tools.

This policy explains the general structure of how NGS conducts the process of responsible vulnerability disclosure to our clients, software vendors, organisations tasked with critical infrastructure protection and the Internet public. This policy intends to enable all parties to understand and address vulnerabilities expeditiously in their environment and to minimize the risks that vulnerability information poses.

All NGS Research Vulnerability Statements are released on the NGS Software Web site <http://www.ngssoftware.com/research/advisories/> for public viewing.

Vulnerability Disclosure Goals

The goals of this policy are as follows:

- To specify the manner in which NGS disclose vulnerability information
- To inform software vendors of the NGS policy regarding disclosure
- To inform the wider internet community of the NGS policy
- To give a rationale for our policy, in the hope that other organisations and individuals adopt a more responsible disclosure policy

Vulnerability Disclosure Process

NGS Research engages in active programs of original Internet and network security research. The disclosure of vulnerability information is provided as a public service to vendors, NGS clients and the general Internet population. The NGS Research vulnerability disclosure process is divided into five logical stages:

- I. Initial Discovery Phase
- II. Vendor Notification Phase
- III. Client Mitigation Phase
- IV. Public Technical Disclosure Phase (Technical Advisory)
- V. Accelerated Disclosure (in exceptional circumstances)

When a vulnerability is discovered, NGS Research uses the following process for initial discovery, notification and public disclosure:

I. Initial Discovery Phase

During the course of our independent research, the NGS team frequently discovers security vulnerabilities. When a vulnerability is discovered, the NGS team investigates the bounds of the vulnerability; including 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.

Investigations are made to ascertain the extent of the vulnerability – in particular previous versions of the software or hardware, other operating system platforms or architectures, the exploitability of the issue and the extent of previous related public disclosures.

If a vulnerability is discovered during a paid engagement, NGS Research works closely with the client on finding a solution, and will not pursue this vulnerability independently without the client's express permission. It is at the client's discretion whether a security advisory procedure will be instigated at the conclusion of the engagement.

At the conclusion of this stage, NGS Research constructs the draft Technical Advisory document.

NGS Research works with the NGS Software team to develop the necessary checks and vulnerability enumeration procedures for the identified vulnerability. This information is then incorporated into the appropriate NGS Software commercial tools.

II. 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. It is the responsibility of NGS Research to aid the vendor in understanding the significance of the discovered vulnerability and to provide any technical aid in developing a serviceable solution that will secure NGS clients and the vendor's customers.

The stages to this vendor notification phase are as follows:

NGS Research establishes communication with the affected vendor(s).

NGS 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.

NGS defines initial communication as any attempt to contact the vendor via an approved email address, telephone number, Fax, or by sending an e-mail to security@, security-alert@, support@, info@, and secure@ vendor - with the relevant information.

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 NGS through the vulnerability disclosure process. NGS prefers to use encrypted email as the communication channel for vulnerability information.

NGS Research formally notifies the vendor of the discovery of the vulnerability and that NGS will distribute information on the schedule outlined in this document.

Initial vendor notification begins when NGS Research sends through a draft of the Technical Advisory to the primary vendor contact.

NGS will work closely with the affected vendor to reproduce the security vulnerability and will make reasonable effort to provide the vendor with information to assist in reproduction of the vulnerability. This may include detailed exploitation information, proof of concept code and any special testing instructions that may be required. NGS Research may also assist in testing vendor supplied patches or workarounds to confirm that the issue has been corrected. This may include liaising with a NGS Consulting client through which the vulnerability may have been originally discovered.

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

The vendor is directed to this policy document.

If the vendor could not be contacted, NGS will continue to attempt to initiate contact with security or development personnel at the vendor concerned. If no response is obtained after repeated attempts, NGS may begin an Accelerated Disclosure process (section V below).

The vendor notification phase proceeds as follows:

- If the vulnerability exists within a supported product, the vendor should reproduce the vulnerability following the information contained within the Technical Advisory, determine if there is enough evidence for the existence of the vulnerability if it cannot be reproduced, determine if the vulnerability is already known (and possibly already resolved), or work with NGS or other security experts to determine if the vulnerability is related to the specific environment in which it was discovered (including configuration errors or interactions with other products). As resources permit, NGS will help the vendor with the validation phase when requested.
- If the vulnerability is found in an unsupported or discontinued product, the vendor may refuse to validate the vulnerability. However, the vendor should undertake measures to ensure that the reported vulnerability does not exist in supported product versions or other supported products based on the vulnerable product.
- The vendor should examine its product to ensure that it is free of other problems that may be similar to the reported vulnerability. Traditionally, related vulnerabilities in the same product are often found by others after a specific vulnerability is publicly disclosed. Finding multiple vulnerabilities beforehand, during the validation phase, saves the vendor and their customers time and money by minimising the need to create and install multiple patches or updates.
- The vendor should provide status updates to NGS Research every 7 days. However, the vendor and NGS Research may come to an agreement for sharing less frequent updates.

There are often valid reasons why vulnerabilities take a long time to resolve. If a good faith effort is being made by the vendor to validate the vulnerability, NGS Research will generally delay the public disclosure of information about the

vulnerability until a resolution is found or created, however NGS reserves the right to begin an accelerated disclosure process at any time.

Some example reasons for accelerated disclosure are noted in Section V of this document.

III. Client Mitigation Phase

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

Release of NGS Software tools updated with vulnerability information

The appropriate NGS Software commercial tools will contain the necessary checks to identify the vulnerability in our clients' environments and also contain workaround/fix information for the vulnerability.

IV. Public Disclosure Phase

Once the vendor has successfully addressed the vulnerability by releasing a patch and/or workaround information, NGS will release a Technical Advisory containing the full technical details of the bug to numerous reputable and approved security mailing lists.

The NGS approved mail distribution lists include:

Bugtraq
NTbugtraq
Vulnwatch

The Technical Advisory includes a management overview of the security vulnerability, information on the impact of the discovered issue, a list of affected product versions, a technical description of the issue that can be used to validate and replicate the issue, recommendations for correcting or mitigating the issue and other relevant vulnerability tracking information.

NGS do not typically release exploit or proof-of-concept code with advisories; however we do 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.

If a new or unusual technique is required to exploit a bug, 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 generally not include functional exploit code, and wherever possible they will be 'sanitised' minimal code examples that illustrate the technique.

Advisory coordination centres notified of the vulnerability

NGS acknowledges that, in order to ensure that the Internet public is informed of the existence of the vulnerabilities in the most efficient and timely manner, we must work closely with a number of specialised advisory coordination centres. Some time prior to public disclosure, our approved list of advisory coordination centres may be issued an electronic copy of the Technical Advisory document and supplementary workaround information.

V. Accelerated Disclosure/Procedural Exceptions

NGS 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:

- The vendor issues a patch or 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.
- NGS Research receives evidence from reliable sources that an exploit is available in the wild.
- The vulnerability is reported by the media.
- The vendor becomes unresponsive.