COORDINATED DISCLOSURE GUIDELINES

NEW ZEALAND INTERNET TASK FORCE

OCTOBER 2014

Start

WHY COORDINATED DISCLOSURE MATTERS:

Our daily lives are becoming more and more reliant on Information and Communication Technology systems (ICT systems), and we all need to have confidence that these systems are secure and robust. Maintaining and enhancing the trust that New Zealanders place in ICT systems is important and challenging. These guidelines are designed, in their own small way, to help make the internet safer and more secure for us all.

We think that the time has come for New Zealand to have some clear guidance on how to both disclose vulnerabilities in ICT systems and to respond to these disclosures in a mature, cooperative way.

We all benefit when information security experts can work together to improve the security of ICT systems across the country. We are a small nation of practically minded, reasonable people. We want to see that part of our national character better applied to the way we work together to identify, disclose and fix ICT vulnerabilities.

Scope of these guidelines

*These guidelines are designed to help anyone who finds a vulnerability in a website or ICT system (a **finder**) and anyone who owns or manages a website or ICT system (an **organisation**).*

Chief information officers, chief information security officers, information technology security managers, hackers, security researchers, system administrators and/or risk officers should all make themselves familiar with the concept of coordinated disclosure.

The New Zealand Internet Task Force

We are a not-for-profit organisation with the mission of *improving the cyber security posture of New Zealand*. The Task Force is a forum based on mutual trust used for debating, networking, information-sharing and collaborating on matters relating to the cyber security of New Zealand.

Our membership comes from the security community across government, law enforcement, academia and private sector industries, including telecommunications, information technology and financial services.

Why we are producing these guidelines

Our mission is to raise the cyber security posture of New Zealand. These guidelines can help improve information security by enabling organisations to become aware of the security vulnerabilities in their ICT systems and fix them.

We also want to enable people who find vulnerabilities to approach ICT system owners in good faith without fear of reprisal. We do not wish to encourage illicit researching of vulnerabilities, but we do want to encourage responsible behaviour when a vulnerability is found – on the parts of both the finder and the organisation that has the vulnerability. We believe organisations should be prepared for when they get a call from a finder and should have processes ready to deal with the situation.

Because the NZITF has a broad membership of security professionals, we think that we can provide guidance that will add value, set some clear boundaries and make it easier for security professionals to work together and help improve cyber security in New Zealand.

Acknowledgements

The Task Force would like to thank the members of the coordinated disclosure working group – in particular *Lateral Security and the National Cyber Crime Centre* – for their contributions and support during the development of these guidelines.

Want to get to the really useful stuff?

Overview of coordinated disclosure

Coordinated disclosure is about people working together, for the benefit of us all, to fix security vulnerabilities that have been identified.

Coordinated disclosure is not just a way that a finder engages with an organisation; it is underpinned by organisations that have good policies and processes. Coordinated disclosure works best when organisations are prepared to respond when a finder contacts them with a vulnerability.

Goals of coordinated disclosure

The main goal of coordinated disclosure is for organisations that run web and ICT systems to take security seriously and respond to reported vulnerabilities by fixing them in a timely fashion. This, in turn:

a) protects the public from security vulnerabilities

b) acknowledges independent finders for their actions and, in particular, for their responsible approach

c) ensures that organisations have enough time to respond to vulnerabilities in a controlled fashion before they are made public.

Principles of coordinated disclosure

Coordinated disclosure is based on four main basic principles:

- Both parties will act in good faith to identify and fix security vulnerabilities.
- Both parties will ensure they act within the law.
- Both parties should be tolerant and patient with one another.
- The vulnerability, and the fact that the finder found it, would ordinarily be made public at the end of the process.

Acting in good faith is very important. For vulnerability disclosure, this means acting in way that is genuine, as transparent as possible and does no harm.

Responsibilities

Everyone is responsible for their own actions. Finders are responsible for their actions and the way in which they discover a vulnerability. Reporting a vulnerability through a coordinated disclosure policy does not mean that legal action cannot be taken against you if you have broken the law.

Under its coordinated disclosure policy, an organisation may agree to not make a criminal complaint, but that is their decision.

Organisations are responsible for the systems that they build. It's best not to react in anger when a finder comes to you with a vulnerability. Sometimes it can be an innocent coding mistake – maybe one of your administrators didn't roll out a patch 100% – or maybe the finder figured out a totally new way of gaining access. Whatever the case, the finder didn't create the vulnerability, they found it.

Why is coordinated disclosure a good thing?

Why should you care about coordinated disclosure? For finders, the answer is because you want:

a) to help fix a potential security problem

b) to avoid an unwarranted police investigation

c) the mana that comes with being recognised as the person who found the vulnerability.

For organisations, embracing coordinated disclosure is good because:

a) your system will have vulnerabilities that you do not know about

b) you want finders to know they can approach you with a vulnerability they find.

Quick help checklist

Finders

Discovering a vulnerability

- ☐ Don't tell anyone (keep knowledge of the vulnerability to yourself).
- ☐ Document the vulnerability (this will help the organisation better understand what the problem is).

Notify the organisation

- ☐ Check to see if the organisation has a coordinated disclosure policy.
- ☐ Report the vulnerability to the organisation in a secure manner.
- ☐ Be clear, concise and professional.
- ☐ Wait to hear back from the organisation.

Investigation & mitigation

- ☐ Provide any additional information requested (within reason).

Publication

- ☐ Work with the organisation on an agreed publication method and timing.

Organisations

Have a coordinated disclosure policy

- ☐ Put in place processes for when you receive a disclosure report.
- ☐ Publish your policy, and a way for finders to contact you, on your website.
- ☐ Make sure you have a PGP key so that finders can communicate with you securely.

Receiving a report

- ☐ Acknowledge receipt of report, thank the finder and inform them of your next steps and timeframes (this is also a good time to find out if they want to publish).

Investigation

- ☐ Triage and assess the vulnerability.
- ☐ Develop a plan how to fix or mitigate the vulnerability, and update the finder.
- ☐ Check your system to see if you have been compromised (if you have been compromised, then you should deal with that separately from the coordinated disclosure process).

Mitigate & fix

- ☐ Test and fix the vulnerability.

Publication

- ☐ Work with the finder to agree how and when to publish.

Coordinated disclosure for organisations

Organisations need to build and publish a coordinated disclosure policy, make it easy for finders to contact you (and communicate with you privately). Developing a policy will help you plan for when a finder contacts you.

Have a coordinated disclosure policy

If you want people to disclose vulnerabilities, then you need a clear, easy to understand policy that you publish on your website.

A published policy and contact details send a signal to finders that not only do you have someone in security that they can contact, but you're also more likely to be responsive to them making contact with you. If you do not publish a coordinated disclosure policy and finders cannot easily get in contact with your security team, then they are not likely to actually contact you about a vulnerability that they find – which leaves you, your business and your clients exposed and vulnerable.

Make it easy for people to report to you

Publish (and monitor) a contact email so that finders can contact your security team. We recommend the simple security@yourorganisation...

You also need some method of having private conversations with the finder. They are contacting you with a vulnerability in your system. Requiring details to be encrypted is a basic security step, to lessen the possibility of someone else finding out about the vulnerability. We recommend using a mechanism for people to communication securely with you (such as PGP) for your private communications with the finder.

Keep the finder updated during the process

Be clear with the finder when you communicate with them. Your first reply (potentially an autoreply) when the finder makes contact should provide a timeframe for when you will contact them next (eg within 2 days). Once you have agreed that there is a vulnerability and you are working to fix it, you should provide them with regular updates – current best practice suggests every 7 days.

It is important that you are clear on how frequent your updates will be from the start. Being consistent and true to your word will help build trust between you and the finder.

Keep your word

Follow through on all the commitments and undertakings that you make to the finder. Being consistent, treating them with respect and keeping your word are all critical ways to build the trust between you and the finder.

Publish an advisory about the vulnerability

Once you have fixed the vulnerability, coordinate with the finder to publish an advisory setting out the nature of the vulnerability, who found it, when it was fixed and any instructions for updating it. Publication is an assumed component of coordinated disclosure. However, sometimes a vulnerability may not warrant public disclosure, and notification to your customers and to other security professionals could be the best way forward. We recommend that some form of publication should be undertaken.

Check to see if the vulnerability has been exploited

As a part of good coordinated disclosure practice, when a finder tells you there is a vulnerability in your system, you should check it to see if the system has been compromised. Remember, the finder has engaged with you in good faith, so you should be doing the same. Assuming they have broken the law and treating them like a criminal is not going to help you fix the vulnerability and is likely to stop other finders from helping you out in the future.

Accepting the risk

Some organisations may want to 'accept the risk' and, rather than fixing the vulnerability, simply put it on the risk register. We recommend against this approach – instead we recommend coordinated disclosure as a good way to uncover and fix vulnerabilities. Remember, hackers do not care about risk registers!

Coordinated disclosure for finders

Reporting a vulnerability is not always easy, especially if you have not done it before. Here is some basic guidance that you should be keeping in mind when trying to disclose a vulnerability.

How to behave

Below is a list of simple tips to help communicate with the organisation and keep yourself out of trouble.

- Disclose as soon as is practical after finding the vulnerability
  Disclosing a vulnerability shortly after finding it shows that you want to do the right thing and get it fixed. Waiting for weeks before disclosing is not a good idea and does not engender trust.
- Keep it secret, keep it safe
  Keep the existence of the vulnerability confidential. Contact the organisation, inform them that you have a vulnerability you want to disclose to them and ask them for a PGP key so you can send them the details. Do not tell anyone else about the vulnerability until after the organisation has fixed it.
- Clearly explain the vulnerability
  Explain the vulnerability so the organisation's security team can understand and replicate it for themselves. Provide whatever evidence you have, declare any data you may have obtained and make sure that you destroy any copies of information you have.
- Make sure you don't blackmail
  Blackmail is making someone perform an act against their will by threatening to disclose information or cause damage. If, during the disclosure process, you say "fix this vulnerability or else I will..." you are probably committing blackmail. If you wish to go public with a vulnerability, make sure your actions are distinct from the actions of the organisation.
- Don't ambulance-chase
  You should not approach an organisation in anticipation of obtaining consultation work with them. That is unprofessional and could lead to allegations of blackmail.

Know the law

In 2003, New Zealand introduced computer crimes dealing with unauthorised access to computer systems. These are now sections 249–252 of the Crimes Act. Nothing in these guidelines removes your responsibility to act within the law. You should make sure you understand the law and act within it at all times.

Who to disclose to?

One issue can be who you should be disclosing the vulnerability to. Many ICT systems and websites use, or rely on, software from other companies. Sometimes it can be hard to tell whether the vulnerability is in their particular instance of the system or in the background database. We recommend that you contact the organisation that owns the website or system where you found the vulnerability. For example, if you find a vulnerability on a university website, exposing student information, you should disclose to the university. Their security team can deal with their vendor as needed.

What if the organisation doesn't reply?

The organisation's website should have some information about how long they will take to get back to you. If you do not hear back from the organisation, you should check that you contacted them in the correct way.

Then, after 60 days of no contact, you could either escalate the situation from the security team to the chief executive, or, if you think the vulnerability is serious enough, you could publish your own advisory (full disclosure).

What if an organisation 'accepts the risk'?

An organisation could decide to 'accept the risk' of the vulnerability to their organisation, including choosing not to fix a particular vulnerability. If the organisation is not going to fix the vulnerability, then the question is whether you walk away or make the vulnerability public (full disclosure).

Full disclosure

If you have disclosed a vulnerability to an organisation which chooses not to act, you could decide to make the vulnerability public without waiting for them. If you do decide to undertake full disclosure, you should consider the seriousness of the vulnerability, the public interest in knowing about the bug, and the harm that publication of an unmitigated vulnerability could cause.

Understand the consequences of your actions and if you do decide to publish the vulnerability, be prepared to deal with the fallout.

What if you want to disclose anonymously?

The default for coordinated disclosure is that finders work directly with organisations. However, in some cases you might not:

a) feel comfortable in approaching them directly but you still want them to know about, and fix, the vulnerability – maybe they don't have a coordinated disclosure policy, or someone you know has had a bad experience in the past with that organisation

b) have heard back from the organisation and you want to escalate the matter before engaging in 'full disclosure'.

It is possible to go through an intermediary to protect your anonymity, either initially or long term. In many countries a Computer Emergency Response Team (CERT) will often act as an intermediary for security researchers (eg FinCERT acted as an intermediary for the security researchers who discovered Heartbleed[1]).

However, New Zealand does not have a designated CERT at this point in time. Therefore, we (the New Zealand Internet Task Force) can receive anonymous vulnerability disclosures and approach the relevant organisation on your behalf.

We undertake to maintain the anonymity of finders who want to remain anonymous. You can find our PGP key on our website www.nzitf.org.nz, and you can email us at disclosure@nzitf.org.nz.

1 Heartbleed is a vulnerability in OpenSSL.
For more information visit: http://heartbleed.com.

Summary

Coordinated disclosure is a relatively simple method and process for finders and organisations to work together to identify, understand and fix security vulnerabilities.

The most important things to keep in mind are:

- both finders and organisations need to act in good faith when dealing with one another
- coordinated disclosure is about solving security vulnerabilities – this should be your focus.

Coordinated disclosure does not have to be hard. If we all cooperate, work together in good faith and remember that we are all working together to make New Zealand's ICT systems more secure, then we should be able to make coordinated disclosure in New Zealand a success.

Other coordinated disclosure resources

If you want to know more about coordinated disclosure – especially if you are building a coordinated disclosure policy yourself – some good resources and examples include:

- ISO 29147 *Vulnerability Disclosure* is dedicated to vulnerability disclosure. You can purchase a copy from NZ Standards (www.standards.co.nz).
- ISO 30111 *Vulnerability Handling* Processes provides guidance for organisations on processes receiving and addressing disclosed vulnerabilities. You can purchase a copy from NZ Standards (www.standards.co.nz).
- BugCrowd (a disclosure and bug bounty service provider) has open source disclosure guidelines which are available on github.[2]
- HackerOne (another disclosure and bug bounty service provider) has plain English vulnerability disclosure guidelines that you may find useful.[3]
- The Netherlands' National Cyber Security Centre has also produced disclosure guidelines, which have been translated into English.[4]
- New Zealand Registry Services has a published vulnerability disclosure policy on its website.[5]

Contact

If you have any questions about these guidelines, you can contact us at info@nzitf.org.nz

2 BugCrowd's guidelines can be found here: https://github.com/bugcrowd/disclosure-policy.

3 HackerOne's guidelines can be viewed here: https://hackerone.com/guidelines.

4 The Dutch guidelines are available in English here: https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

5 You can view NZRS's disclosure policy here: https://nzrs.net.nz/about/vulnerability-disclosure-policy

disclosure@nzitf.org.nz
www.nzitf.org.nz | info@nzitf.org.nz
PO Box 11-881 Thorndon, Wellington 6142