Effective Security Response

*Lessons learned from the XenProject security response process*
Our software has bugs.

Our software has security bugs.
Our software has bugs.

Our software has **security** bugs.

When you discover bugs, your **security**
When you discover bugs, your security response process will have a major impact on how much risk your users are exposed to.
You can't have *no* security response process;

You can only have a *good* one or a *bad* one.
You can't have *no* security response process;

You can only have a *good* one or a *bad* one.
You can only have a **good** one or a **bad** one.

XenProject's security response process
Goals
Theory

Goals

No disclosure

Privately vulnerable

Full disclosure

Publicly vulnerable

Coordinated / Responsible disclosure

Reporter reports a vulnerability
Coordinate a disclosure
Release of vulnerability
No disclosure
absence of evidence
and
evidence of absence
Full disclosure
Privately vulnerable

Publicly vulnerable
Privately vulnerable

Publicly vulnerable
Coordinated / Responsible disclosure
Reporter reports bug to software vendor
Coordinate a date for public disclosure
Release of vulnerability and binary fix
Reporter reports bug to software project
Coordinate a date for public disclosure

Project sends patch to pre-disclosure list
Release of vulnerability, patch, and binary fixes
Honor the wishes of the reporter

Include a suggested disclosure timeline
Honor the wishes of the reporter

Include a suggested disclosure timeline
Experience

XSA-7

XSA-108
XSA-7

Individual address on the pre-disclosure list

Require an alias to a security team

Pressure put on management chain
Individual address on the pre-disclosure list

Require an alias to a security team
Individual address on the pre-disclosure list

Require an alias to a security team
XSA-7

Individual address on the pre-disclosure list

Require an alias to a security team

Pressure put on management chain
Pressure put on management chain

Talk to your management chain ahead of time

Diversity in your organization
Pressure put on management chain

Talk to your management chain ahead of time

Diversity in your security team
Pressure put on management chain

Talk to your management chain ahead of time

Diversity in your security team
XSA-7

Coordinated / Responsible disclosure

Individual address on the pre-disclosure list

Require an alias to a security team

Pressure put on management chain
Putting pressure directly on the reporter

Only credit in the public disclosure
Putting pressure directly on the reporter

Only credit in the public disclosure
XSA-7

Coordinated / Responsible disclosure

Individual address on the pre-disclosure list

Require an alias to a security team

Pressure put on management chain
Principle and practicality
Unfairness

Users don't know that an update is
Users don't know that an update is coming

Announce existence of a vulnerability and the public disclosure date
Users don't know that an update is coming ahead.

Announce existence of a vulnerability and the public disclosure date.
Media speculation storm

Handling a slew of applications
Media speculation storm

Handling a slew of applications

Make the process mechanical
Handling a slew of applications

Make the process mechanical

Are service providers allowed to deploy updates during an embargo?
Make the process mechanical

Are service providers allowed to deploy updates during an embargo?

What can service providers say?
Are service providers allowed to deploy updates during an embargo?

What can service providers say?

Can software providers provide binaries to service providers?
What can service providers say?

Can software providers provide binaries to service providers?
Questions?

_XenProject Security Response Process_
http://www.xenproject.org/security-policy.html

*Feedback / questions / comments*: george.dunlap@citrix.com
Effective Security Response

Lessons learned from the XenProject security response process