Our software has bugs.

Our software has **security** bugs.

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 respo

You can only have a *good* one or

XenProject's security res

Goals

Effective Security Response

Theory

Lessons learned from the XenProject security response process

Experience

XSA-7

XSA-108

Questions?

Our software has bugs.

You

Our software has **security** bugs.

Our software has bugs.

You

You

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

Xen Project's security response process

Goals

No di

impact on how much risk your users are exposed to.

onse

Goals

No disclosure

absence of evidence
and
evidence of absence

Theory

Privately vulnerable

Full disclosure

Publicly vulnerable

Coordinated / Responsible disclosure

Reporter report
Coordinate a da
Release of vuln

No disclosure

absen

evider

absence of evidence

and

evidence of absence

Privately vulner

Full disclosure

Publicly vulnera

Privately vulnerable

Publicly vulnerable

Privately vulnerable

Publicly vulnerable

Coordinated / Responsible disclosure

Rep

Coo

Rele

Reporter reports bug to software vendor

Coordinate a date for public disclosure

Release of vulnerability and binary fix

Rep

Coo

Pro

Rele

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

ject

Coordinated / Responsible disclosure

Experience

XSA-7

Individual address on the p
disclosure list

Require an alias to a securi

XSA-108

Pressure put on manageme

Talk to your management
of time

Diversity in your security t

Coordinated / Responsible disclosure

Repo
Coor
Relea

XSA-7

Individual address on the pre-disclosure list

Require an alias to a security team

Pressure put on management chain

ce

Individual address on the pre-disclosure list

Princi

Require an alias to a security team

Individual address on the pre-disclosure list

Princi

Require an alias to a security team

Unfair

Coordinated / Responsible disclosure

Repo
Coor
Relea

XSA-7

ce

Individual address on the pre-disclosure list

Require an alias to a security team

Pressure put on management chain

Unfair

Pressure put on management chain

Talk to your management chain ahead of time

Users

comin

Annou

and th

Pressure put on management chain

Talk to your management chain ahead of time

Diversity in your security team

Users
comin

Annou
and th

Pressure put on management chain

Talk to your management chain ahead of time

Diversity in your security team

Users
comin

Annou
and th

Coordinated / Responsible disclosure

Repo
Coor
Relea

XSA-7

ce

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

Coordinated / Responsible disclosure

Repo
Coor
Relea

XSA-7

ce

Individual address on the pre-disclosure list

Require an alias to a security team

Pressure put on management chain

Principle and practicality

m

Principle and practicality

m

Unfairness

ain

Users don't know that an update is

Unfairness

ain

ahead

Users don't know that an update is coming

Announce existence of a vulnerability and the public disclosure date

ain

ahead

Users don't know that an update is coming

Announce existence of a vulnerability and the public disclosure date

ject

Coordinated / Responsible disclosure

Experience

XSA-7

Individual address on the p
disclosure list

Require an alias to a securi

XSA-108

Pressure put on manageme

Talk to your management
of time

Diversity in your security t

Experience

XSA-108

Media speculation storm

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?

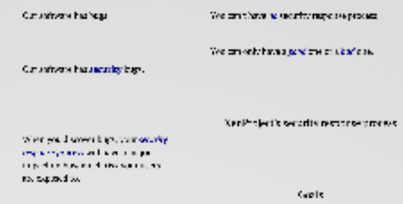
XenProject Security Response Process

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



Theory

Experience

XSA 7

XSA 108