Our software has bugs.

You can't have no security respo

You can only have a good one or

Our software has security bugs.

XenProject's security re-

When you discover hugs, your security response process will have a major impact on how much risk your users are exposed to.

200

Effective Security Response

Theory

Lessons learned from the XenProject security response process

Experience

XSA-7

Our software has bugs.

You

You

Our software has security bugs.

You

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 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.

Tou call offiny flave a good offe of a bud offe.

XenProject's security response process

Actification and accountly response process

Goals

No di

impact on how much risk your users are exposed to.

Goals

nse

No disclosure

absence of eviden and evidence of absen

Theory

Full disclosure

Publicly vulnerable

Privately vulnerable

Coordinated / Responsible disclosure

Reporter repor Coordinate a da Release of vuln

No disclosure

abser

evidei

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

Coc

Rel

Reporter reports bug to software vendor Coordinate a date for public disclosure Release of vulnerability and binary fix Rep Coo Pro 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

ILLI

Coordinated / Responsible disclosure

Experience

XSA-7

disclosure list

Individual address on the p

Require an alias to a securi

Pressure put on manageme

Talk to your management of time

Diversity in your security t

XSA-108

Repo Coor Relea

ce

XSA-7

Individual address on the predisclosure list

Require an alias to a security team

Pressure put on management chain

Individual address on the predisclosure list

Princi

Require an alias to a security team

__ _ _

Individual address on the predisclosure list

Princi

Require an alias to a security team

Unfai

XSA-7

Individual address on the predisclosure 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

Annou

and th

Pressure put on management chain

Talk to your management chain ahead of time

Diversity in your security team

Users

Annou

I ressure put off management chair

Talk to your management chain ahead of time

Diversity in your security team

Users

Annou and th

XSA-7

Individual address on the predisclosure 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

Individual address on the predisclosure list

Require an alias to a security team

Pressure put on management chain

Principle and practicality

m

I Illicipic alla practicality

m

Unfairness

ain

Users don't know that an update is

Ollialilicos

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

IUUL

Coordinated / Responsible disclosure

Experience

XSA-7

disclosure list

Individual address on the p

Require an alias to a securi

Pressure put on manageme

Talk to your management of time

Diversity in your security t

XSA-108

Lybellelle

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

Cartestown has begun We continue a secrety repose process . Veg can only have a gard one of a barface. Car software has according bugs. XenPhojert's serurity response process. repairs and a simple transfer of the second second

XSA-7

Effective Security Response

Lessons learned from the XenProject

Theory

security response process

Experience

XSA-108

Hardings developpinglessors

Media specialization aroun-

Was an errich profile (1927)

 $\rm RH\,disdosure$

Na obsilovane

Private valuable

AND volumble

disas a militar

and Address of Green to

Creshund (Report to distress) lapotarrapea seg wadings reads: Gradunes instructive fixianus Relevants i entitiyanti i enyik

Principle and probability

Resentence in the month were project. Our manager is to first a first term on Project sends paid to provide described for its transmitting parts and described

In the formula exposit a sec-orac case for Regular an all some a security team.

Pressure place in an agreement thanks Beershoftlens between kits-A minimum series convenient administration of the χ -model σ and the distribution of the σ

Principles or healt, or the resource Colymplets the publication are

Diseasely in your security out in

Concrete vistas of the reports:

In the same growth for lower of the state.

A communication of the same of