RVASec 2015
Vulnerability Coordination and Concurrency
Allen D. Householder
@__adh__

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Vulnerability Coordination and Concurrency

Introduction & Motivations

Survey of Vulnerability Disclosure Models

Modeling Coordination as Concurrency

What We’ve Learned (So Far)

Conclusion
CERT Advisory
December 1988

ftpd vulnerability

1) Check that you are using version 5.59 of sendmail with the debug option DISABLED. To verify the version try the following commands. Use the telnet program to connect to your mail server. Telnet to your hostname or localhost with 25 following the host. The sendmail program will print a banner which will have the version number in it. You need to be running version 5.59. Version 5.61 will be released on Monday 12/12/1988. Any version less than 5.59 is a security problem.

The following is a sample of the telnet command.

% telnet localhost 25
Trying...
COMMISSIONERS: Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeney

In the Matter of

Fandango, LLC,
a limited liability company.

COMPLAINT

The Federal Trade Commission, having reason to believe that Fandango, LLC (“respondent”) has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Fandango, LLC (“Fandango”) is a Delaware limited liability company with its principal office or place of business at 12200 W. Olympic Boulevard, Suite 400, Los Angeles, CA 90064.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.
15. From March 2009 to March 2013, the Fandango Movies application for iOS failed to validate SSL certificates, overriding the defaults provided by the iOS APIs.

16. Before March 2013, Fandango did not test the Fandango Movies application to ensure that the application was validating SSL certificates and securely transmitting consumers’ credit card and personal information. Although Fandango claimed to have a publicized and effective channel for receiving security vulnerability reports, “Fandango does not have a clearly publicized and effective channel for receiving security vulnerability reports, and instead relies upon its general Customer Service system to escalate security vulnerability reports to the proper employees.”

18. After Commission staff contacted respondent, Fandango tested the Fandango Movies application for iOS and confirmed that the application failed to validate SSL certificates. Fandango discovered that the vulnerability also affected a separate iOS movie ticketing application.
**Issue 118: Windows: Elevation of Privilege in ahsache.sys/NtApphelpCacheControl**

62 people starred this issue and may be notified of changes.

**Status:** Fixed

**Owner:** fors...@google.com

**Closed:** Jan 14

**Cc:** project....@google.com

**Vendor:** Microsoft

**Product:** Windows-Kernel

**Severity:** High

**Finder:** forshaw

**Reported:** 2014-Sep-30

**CCProjectZeroMembers**

**Deadline-90**

**MSRC-20544**

**PublicOn:** 2014-Dec-29

**Deadline-Exceeded**

**CVE-2015-0002**

**Fixed:** 2015-Jan-13

**Project Member**

**Reported by fors...@google.com, Sep 30, 2014**

**Platform:** Windows 8.1 Update 32/64 bit (No other OS tested)

On Windows 8.1 update the system call NtApphelpCacheControl (the code compatibility data to be cached for quick reuse when new processes are created cannot add new cached entries as the operation is restricted to Admin AvcVerifyAdminContext.

This function has a vulnerability where it doesn't correctly check the token if the user is an administrator. It reads the caller's impersonation token, does a comparison between the user SID in the token to LocalSystem's SID in the token so it's possible to get an identify token on your thread from the LocalSystem. For this purpose the PoC abuses the BITS service and COM to get the identity ways.

It is just then a case of finding a way to exploit the vulnerability. It auto-elevate executable (say ComputerDefaults.exe) and sets up the call which forces a RedirectExe shim to reload regsvr32.exe. However any exploit finding a suitable pre-existing app compat configuration to abuse.

It's unclear if Windows 7 is vulnerable as the code path for update has like depending on the flags this might be bypassable. No effort has been put a bug in VNC. It is just using VNC auto-elevation for demonstration.
"Google ... released ... two days before our planned fix"
“We now have a 14-day grace period”
Motivations

Resurgent disclosure kerfuffles

Proliferation of novice vendors

- There are more new vendors than there is vulnerability coordination experience to go around

- Networked services bolted onto existing products
  - cars, refrigerators, door locks, light bulbs, medical devices, industrial control systems

- Anyone can become an app creator
Motivations

Vul markets & bug bounties change the flow of information
See also Katie Moussouris @ OWASP AppSec 2015 https://youtu.be/IPTYYg0OzYQ

Third party libraries are more important than ever
  • Yet library vuls are significantly harder to coordinate well
    See also Kymberlee Price & Jake Kouns @ DerbyCon 4 https://youtu.be/sLxcOtEfGvg

Rampant growth in both awareness of security and the security industry itself
  • Vul disclosure discussions are older than today’s participants
    - “Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done.” – A.C. Hobbs, 1853 (HT: Matt Blaze, Steve Bellovin)
“We now have multiparty, multifaceted coordination needs. These are cross-industry requirements, which means we need to now consider phasing our disclosures. This requires us to open the genie box and **reconsider our approach in a more organized manner**. No longer can a researcher jump out and save the Internet from itself, since its complexity is beyond that stage. A researcher may understand the bug, but **the system of systems and the interactions require a broader group effort**.”

- Peter Allor, Federal Security Strategist, IBM Security

Motivations

“We now have multiparty, multifaceted coordination needs. These are cross-industry requirements, which means we need to now consider phasing our disclosures. This requires us to open the genie box and reconsider our approach in a more organized manner. No longer can a researcher jump out and save the Internet from itself, since its complexity is beyond that stage. A researcher may understand the bug, but the system of systems and the interactions require a broader group effort.”

- Peter Allor, Federal Security Strategist, IBM Security

Modeling the Process
Why Create Models?

Models enable conversations about the process
• without devolving into arguments over the specifics of individual disclosures.

Models can be subjected to analysis
• and are easier to change than day-to-day operations.

Models promote learning and knowledge transfer
• by removing unneeded detail

Reasoned disagreement about a model leads to better models.
Other models

Arbaugh, Fithen, McHugh (2000)

Christey, Wysopal (2002)


draft-christey-wysopal-vuln-disclosure-00.txt
“Responsible” Disclosure?

*Responsible* implies a value judgment

…which turns it into an argument over competing perspectives

*Coordinated Disclosure* is our preferred term

…but that doesn’t always mean wait for the vendor to release a patch
“You're going to find that many of the truths we cling to depend greatly on our own point of view”

Figure 1: Vulnerability Resolution Process Life Cycle

Other models

https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf

Chambers, et al.

Other models

Figure 1. Basic Steps in the Security Vulnerability Reporting and Response Process

Figure 2. Steps in Discovery Phase

Figure 3. Steps in Notification Phase

Figure 4. Steps in Investigation Phase

Figure 5. Steps in Resolution Phase

Figure 6. Steps in Release Phase

http://www.oisafety.org/
"as long as the vendor does not internalize the entire user loss, the vendor will release the patch later than is socially optimal, unless threatened with disclosure."

"The more responsive the vendor is to user losses, the more aggressive the social planner can be by setting a shorter protected period."

"In general, both an instant disclosure and a secrecy policy are suboptimal, although numerical simulations suggest that instant disclosure is particularly inefficient."

The Wolves of Vuln Street (2015)

Other models


Moussouris, Siegel, Houghton, & Ellis
What’s missing from prior models?

Early models were primarily narrative, prescriptive advice

- Many imply more synchronization than we observe in the wild
- “We rarely encounter cases with CERT/CC’s preferred ordering” - Arbaugh, et al. (2000)

Later models start to incorporate

- social cost
- participant motives
- money and markets

But they don’t illuminate how and why coordinated vulnerability disclosure can fail
Modeling the Process

Concurrency
Why Create a Concurrency Model?

Vulnerability disclosure is a multiparty, human-centric, concurrent process
- Vendors
- Researchers
- Coordinators
- Other stakeholders
  - Service providers
  - Governments
  - Users

Each party represents a complex interaction of many people, processes, policies, and procedures
Intro to Petri Nets

Used to model distributed processes as a network of nodes and arcs.
Nodes can be either places (circles), or transitions (boxes).

Arcs (arrows) connect places to transitions and vice versa.
- Places can't connect to places
- Transitions can't connect to transitions

All Petri Net diagrams in this presentation were created using WoPeD
http://www.woped.org/
Places can hold *tokens*, which mark the state of a process.

Transitions represent events that change the state of the process.

- A transition can *fire* when all the places immediately upstream of it are occupied by tokens (i.e., when it is *enabled*).
- When a transition fires, it consumes tokens from its inputs and places tokens in its outputs.
A Simple Model

\[
\begin{align*}
\text{vul exists} & \quad \rightarrow \quad \text{stuff happens} & \quad \rightarrow \quad \text{Public aware of fix} \\
& \quad \rightarrow \quad \text{other stuff happens} & \quad \rightarrow \quad \text{Public aware of vul}
\end{align*}
\]
A Simple Model
A Simple Model
A Simple Model
A Simple Model

Oh No!
0-Day!
Vendor Model

vul exists

V discovers vul

V aware of vul

V studies vul

V ready to write

V writes doc

V ready to publish

V ready to fix

V creates fix

V has fix

V publishes

Public aware of fix

Public aware of vul
Vendor Model
Vendor Model

- Vul exists
- V discovers vul
- V aware of vul
- V studies vul
- V ready to write
- V writes doc
- V ready to publish
- V ready to fix
- V creates fix
- V has fix
- V publishes
- Public aware of fix
- Public aware of vul
Vendor Model

vul exists

V discovers vul

V aware of vul

V studies vul

V ready to write

V writes doc

V ready to publish

V ready to fix

V creates fix

V has fix

V publishes

Public aware of fix

Public aware of vul
Vendor Model
Vendor Model
Vendor Model

What if the vendor publishes report before fix?
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model

Rewind to the decision to notify the vendor
Vendor + Researcher Model
Researcher gives up on vendor, Vendor thought it was fixed

“A combination of mis-communication and lack of testing led to this situation today, hopefully it can be a good learning experience.”
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor + Researcher Model
Vendor, Researcher, Coordinator
Vulnerability Coordination and Concurrency
June 4, 2015

Vendor, Researcher, Coordinator
Vendor, Researcher, Coordinator
Vendor, Researcher, Coordinator

Vulnerability Coordination and Concurrency
June 4, 2015
© 2015 Carnegie Mellon University
Vendor, Researcher, Coordinator
Vendor, Researcher, Coordinator
But this is still just a single vendor vulnerability
Multivendor, researcher, coordinator, miscreant
Multivendor, researcher, coordinator, miscreant

HOW ABOUT NO
Limits of Concurrency Modeling using Petri Nets

It’s hard to present this stuff in a way that is understandable once you get so many interactions

State space grows quickly and the model becomes unwieldy

Hard to model history as it evolves

• E.g., when something different happens based on whether you passed through some particular node on the way here

Agent-based models seem promising since they can basically model a state machine per participant and the interactions between them
Other Ways to Think About It: State Machines

unaware

learn about vul

awaiting external event

active

publish

stop work

disengage

resume

re-engage

wait

stall

disengaged

done

abandon
Modeling Helps You Reason About a Bigger World
What we’ve learned so far

Things that break
Humans

Have

• Knowledge
• Motives (fortune, fame, altruism, challenge, spite, pride, etc.)
• Limited attention
• Emotions
• Biases
• Perceptions
• Expectations

All of these affect decisions and actions

See also Katie Moussouris @ RSA 2013 Flash Talk https://youtu.be/T6e70upcfI4
## Researcher / Vendor Communications

**Channel is never established**
- Can’t find vendor contact
- Contact is nonresponsive

**Receiver saturates / Channel capacity exceeded**
- Usually on recipient end
- Human-process / cognitive load

**Channel breaks down**
- Synchronization is lost
- Mismatched expectations
- One side goes nonresponsive
- One side goes hostile

**Chilling effects of prior behavior & experience**
- See also *iterated prisoner’s dilemma strategies*
  - Nice, retaliating, forgiving, non-envious

[See also](https://en.wikipedia.org/wiki/Prisoner’s_dilemma)
One Vendor, Many Vuls

Fuzzing + uniqueness + exploitability analysis = vulplosions

CERT BFF & FOE (fuzzers) highlighted bottlenecks in our own processes and in vendor vul coordination capacity

msg6333 (view)

Author: reimar

Date: 2009-07-03.11:55:02

On Tue, Jun 30, 2009 at 06:28:54PM +0000, WD wrote:
> Attached is a zip file with multiple (73) files that cause ffmpeg to crash.

A lot of these file crash no longer with SVN, please get rid of those that work now, 73 files are simply too much to handle.
Many Vendors, One Vul (Type A)
Heartbleed draws attention to OpenSSL disclosure policy

“The more people you tell in advance the higher the likelihood that a leak will occur. We have seen this happen before, both with OpenSSL and other projects.”

[Maintaining vendor contacts] “is a significant amount of effort per issue that is better spent on other things.”

“We have previously used third parties to handle notification for us including CPNI, oCERT, or CERT/CC, but none were suitable.”

“It's in the best interests of the Internet as a whole to get fixes for OpenSSL security issues out quickly. OpenSSL embargoes should be measured in days and weeks, not months or years.”

https://www.openssl.org/about/secpolicy.html
Many Vendors, One Vul (Type B)
CERT Tapioca and the Android SSL MitM avalanche

Find one vul in lots of things, in parallel, as fast as you can

https://www.rsaconference.com/events/us15/agenda/sessions/1638/how-we-discovered-thousands-of-vulnerable-android
Questions We’ve Asked Ourselves

How do you sustainably notify hundreds of vendors per day for 5 months?

- Use email contact from app store, no attempt at crypto
- Frustrated known vendors because we didn’t notify their established security contact

Does the “45 Day Rule” apply to SSL MitM vuls?

- In this case, the attacker doesn’t get to pick which apps you use, but you do. (Advantage is to the defender.)
  - Plus, MitM already happening (“Active exploitation” policy clause)
- Originally no advance warning
  - Changed to 7 day advance warning based on vendor feedback

How do you publish 23,000 vulnerability records?

- Used a Google Drive Spreadsheet, our own publishing system couldn’t do it easily
Things that break at scale

CVE?

Total apps tested 1000462
Total apps that have failed dynamic testing: 23667
Many Vendors, Many Vuls

Vulnerability Note VU#317350
ISC DHCP contains a stack buffer overflow vulnerability in handling log lines containing ASCII data.

CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)

Original release date: February 12, 2002
Last revised: Aug 18, 2003
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Products from a very wide variety of vendors may be affected. See Vendor Information for details from vendors who have provided feedback for this advisory.

In addition to the vendors who provided feedback for this advisory, a list of vendors whom CERT/CC contacted regarding these problems is available from

http://www.kb.cert.org/vuls/id/854306
http://www.kb.cert.org/vuls/id/107186

Many other systems making use of SNMP may also be vulnerable but were not specifically tested.

Overview

Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. These vulnerabilities may

Vulnerability Note VU#488682
Intercepting proxy servers may incorrectly rely on HTTP headers to make connections

Original Release date: 23 Feb 2009 | Last revised: 28 Sep 2009
What we’ve learned so far

Things that work
Advice for Vendors

Clear and findable instructions for reporting vulnerabilities

- An email address (security@example.com)
- Web forms, bug report systems are okay too
  - if they allow easy marking of security issues

Acknowledge receipt of reports quickly

Set expectations clearly
Advice for Vendors

Maintain open communication channel with vulnerability reporters
• Occasional “We’re still working on it” notes can keep things from going sideways

Offer a bug bounty
• Be careful to incentivize the right things at the right times

Don’t sue (or threaten to sue) researchers
• Publicity works in counterintuitive ways

Have a “cooperation bias”
Advice for Researchers

Attempt to contact the vendor before going public
• If you can’t find vendor contact or vendor is not responsive, contact a coordinator (like CERT/CC)

Provide clear and concise reports
• Steps to reproduce, proof-of-concept code if possible

If you have constraints, articulate them upfront
• Conference publication deadlines, etc.

Give vendor a final warning before publishing
• Waiting for the vendor is not always possible
Advice for Researchers

Don’t assume the vendor is ignoring you intentionally
- Tickets get closed by mistake
- People change jobs
- Priorities shift
- Errors happen

Know your rights
https://www.eff.org/issues/coders/vulnerability-reporting-faq

Have a “cooperation bias”
Conclusion
Average stats (like vul reports/year) hide the structure of the vul coordination picture and can mislead you into thinking that the effort involved is trivial.

It’s not.

You don’t build storm sewers to handle your average daily rainfall.

You build capacity for the worst flood you expect over a given timeframe.

And sometimes you’ll be wrong.
There Is No One-Size-Fits-All Disclosure Policy

Traditional shrink-wrapped software

Enterprise customization

Continuous deployment

Mobile apps, App stores

Cloud services (IaaS, PaaS, SaaS)

Embedded devices and smart things
If you have a vulnerability, if no one else can help...

Multiple vendors needed to fix
- Internet Infrastructure
- Third-party libraries

Bug bounties may not apply
- The vendor doesn’t offer one
- The terms are unacceptable (or payouts are lame)
- You’re otherwise ineligible

Vendor problems
- Non-responsive vendors
- Hostile vendors
  - or fear thereof

Desire to remain anonymous
- Either during disclosure process or long-term
...and you can find them...

https://forms.cert.org/VulReport
...maybe you can coordinate with

Software Engineering Institute
Carnegie Mellon University
For more information

https://www.eff.org/issues/coders/vulnerability-reporting-faq


https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm


ISO/IEC 29147 Information technology -- Security techniques -- Vulnerability disclosure [Externally focused]

ISO/IEC 30111 Information technology -- Security techniques -- Vulnerability handling processes [Internally focused]
Contact me

Allen D. Householder
Email: adh at cert dot org
Twitter: @__adh__