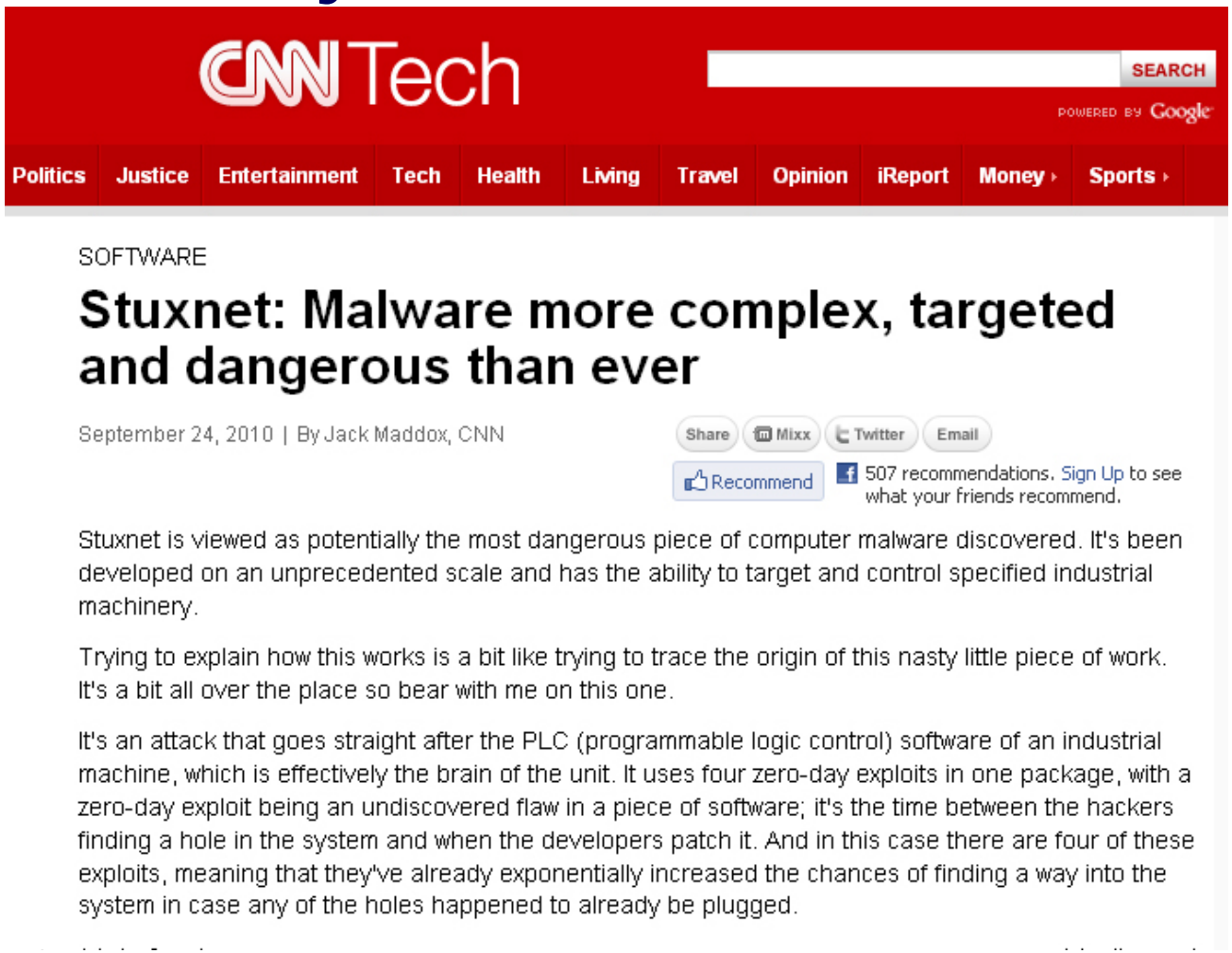
ICS Vulnerability Disclosure

To Disclose or Not to Disclose

ICS-CERT
Control Systems Security Program
U.S. Department of Homeland Security

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS Security Entered the Public Stage



CNN Tech

SEARCH

POWERED BY Google

Politics | Justice | Entertainment | Tech | Health | Living | Travel | Opinion | iReport | Money | Sports

SOFTWARE

Stuxnet: Malware more complex, targeted and dangerous than ever

September 24, 2010 | By Jack Maddox, CNN

Share | Mixx | Twitter | Email

Recommend | 507 recommendations. Sign Up to see what your friends recommend.

Stuxnet is viewed as potentially the most dangerous piece of computer malware discovered. It's been developed on an unprecedented scale and has the ability to target and control specified industrial machinery.

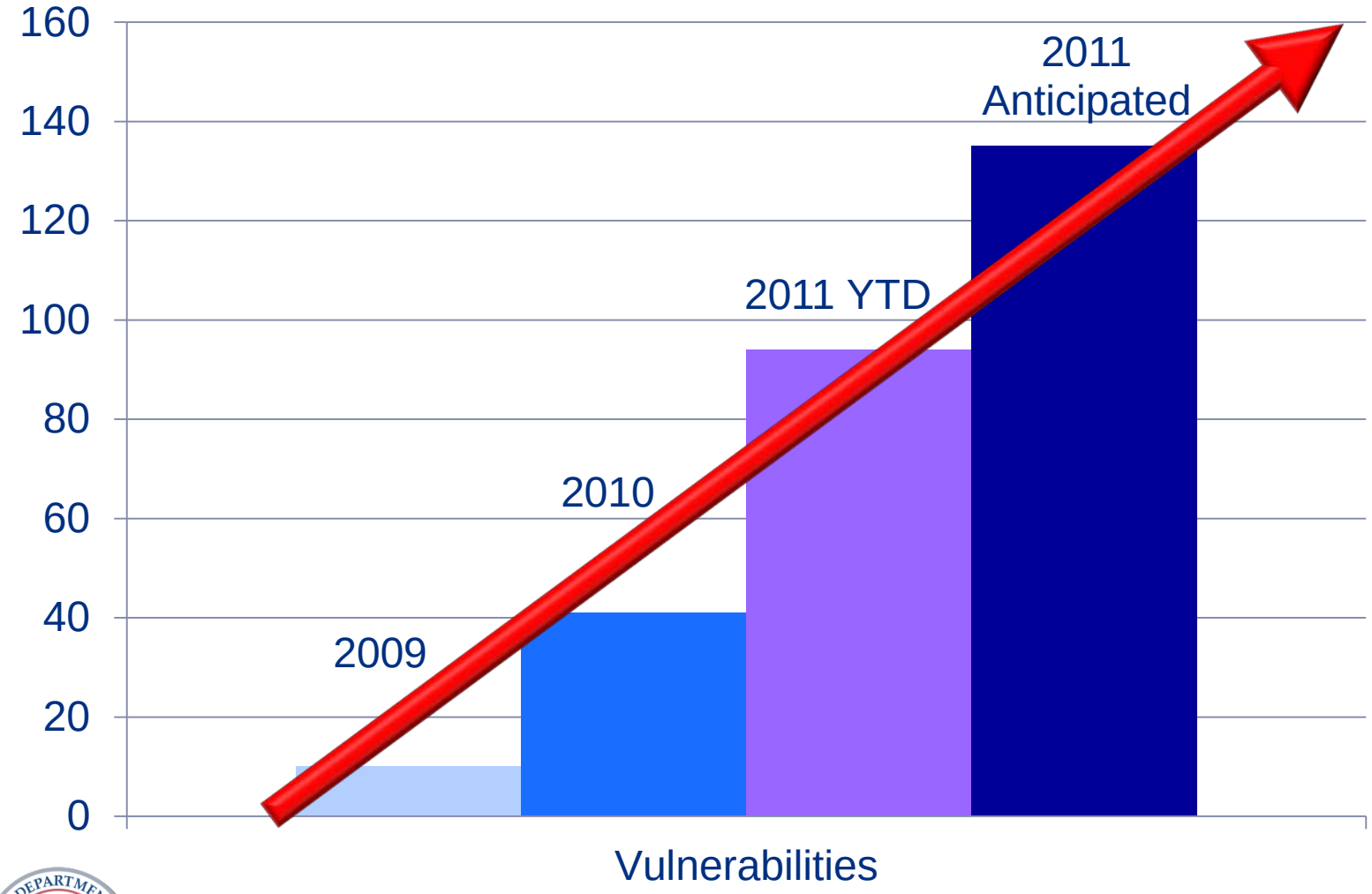
Trying to explain how this works is a bit like trying to trace the origin of this nasty little piece of work. It's a bit all over the place so bear with me on this one.

It's an attack that goes straight after the PLC (programmable logic control) software of an industrial machine, which is effectively the brain of the unit. It uses four zero-day exploits in one package, with a zero-day exploit being an undiscovered flaw in a piece of software; it's the time between the hackers finding a hole in the system and when the developers patch it. And in this case there are four of these exploits, meaning that they've already exponentially increased the chances of finding a way into the system in case any of the holes happened to already be plugged.

Pace for ICS Vulnerability Disclosure is Quickening

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Reported ICS Vulnerabilities



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Who is Disclosing Vulnerabilities?

- ICS vendors
- Reporters from undisclosed sources
- Security researchers
  - Most new vulnerability reports have been from researchers without a control systems background

More Security Researchers are Getting in the Game

- Researchers with an interest in ICS are increasing their work on control system vulnerabilities
- Researchers with no background in control systems have started looking at control system products and finding vulnerabilities
- Researchers who wear hats with a range of colors have all started paying attention to ICS vulnerabilities

Who are the Researchers?

Researchers come from various backgrounds and from a wide range of countries.

Why Do Security Researchers Report Vulnerabilities?

- Improve the security of industrial control systems
- Desire for vendors to write better code
- Passion for hunting for and finding vulnerabilities
- Report vulnerabilities found during security assessments
- Reputation building for name recognition or promotion of consulting services
- Financial reward

Zero-Day Market

- **Buyers**
  - Nation-States
  - Underground Market
  - Commercial Buyers
    - Zero-Day Initiative (TippingPoint)
    - iDefense
  - Vendors–bug bounty programs
- **Brokers** *between Researchers and buyers*
- **Products that contain zero-day exploits**
  - Argeniss
  - Immunity
  - GLEG

GLEG Agora SCADA+ Exploit Pack

- Immunity's CANVAS is a penetration framework similar to the popular Metasploit tool
- GLEG is a small company based in Moscow, Russia, that produces add-on exploit packages for CANVAS
- March 15, 2011, GLEG Ltd. announced the Agora SCADA+ Exploit Pack
- March 25, 2011, GLEG announced it would be adding exploits for the 35 vulnerabilities released by Luigi Auriemma on March 21, 2011
- ICS-CERT has issued two Alerts warning of the availability of this exploit pack and a subsequent update

Agora SCADA+ Pack

GLEG Website:

- “This is an attempt to collect ALL publicly available SCADA vulnerabilities in one exploit pack.”
- “SCADA and related vulnerabilities are very special due to its sensitive nature and possible huge impact involved to successful exploitation.”
- “SCADA Systems are also ‘hard to patch,’ so even old vulnerabilities are actual.”

The Agora SCADA+ Pack features

GLEG Website:

Growing value

- “Due to low real systems patch rank 100% public SCADA vulns coverage”
- “Including old and newly discovered bugs 0 Days for SCADA”
- “We conduct our own in depth research focused on Industrial software & hardware environment”
- “Not only SCADA, but also Industrial PCs, smart chips, and industrial protocols are reviewed. Weak points analyses”
- “Many industrial things suffer from weaknesses like hardcoded password and etc.”

Agora SCADA+ Pack

- GLEG and Immunity have both told ICS-CERT that they have no plans to release any vulnerability details regarding the Agora SCADA+ exploit pack
- At least two ICS vendors have purchased software from GLEG
- GLEG has agreed to notify ICS-CERT of any future product updates
- Cost of licenses (Total 1 year: **$8,930**)
  - Immunity CANVAS 1-year license: $3,530
  - GLEG Agora SCADA+ Exploit Pack 1 year: $5,400

Why are Researchers Targeting Specific ICS Products?

- **Accessibility of ICS Software**
  - Products are often identified by researchers doing a Google search for SCADA software and finding evaluation versions
- **Product Reexamination (copycat)**
  - Researchers often see public disclosures of vulnerabilities in product X, and follow up by downloading product X and finding additional vulnerabilities

Product Reexamination Example

Ecava IntegraXor

Ecava is a small Malaysia-based company. IntegraXor is a web-based HMI used in factory and process automation

- **October 4, 2010,** Jeremy Brown **coordinated** a buffer overflow
- **December 12, 2010,** Luigi Auriemma posted to exploit-db.com details about a directory traversal vulnerability
- **December 21, 2010,** Dan Rosenberg with Virtual Security Research **coordinated** an unauthenticated SQL vulnerability
- **December 22, 2010,** Mister Teatime posted a DLL hijacking vulnerability to OSVDB.org
- **April 12, 2011,** Knud with nSense **coordinated** multiple XSS vulnerabilities

Luigi Auriemma's Disclosures

- October 15, 2010, RealWin Buffer Overflow **Unanticipated**
- December 8, 2010, Wonderware InBatch Buffer Overflow **Unanticipated**
- December 21, 2010, Ecava Integraxor Directory Traversal **Unanticipated**
- December 22, 2010, Sielco Sistemi Winlog Stack Overflow **Coordinated**

- March 21, 2011, Siemens Tecnomatix FactoryLink **Unanticipated**
- March 21, 2011, Iconics Genesis **Unanticipated**
- March 21, 2011, 7-Technologies IGSS **Unanticipated**
- March 21, 2011, RealFlex RealWin **Unanticipated**

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Luigi's Media Attention

digital bond

Advertise He

What's Hot: Bandolier Portaledge Quickdraw SCADA IDS Vulnerability Disclosure

Interview with Luigi Auriemma of 34 0day ICS Vulnerabilities

Dale G Peterson

Tweet 27

Luigi Auriemma, of **yesterday's 34 0day ICS vulnerabilities**, was kind enough to answer some questions we had. I would have preferred a podcast, but neither my Italian nor his English allowed that. I have slightly edited his responses for English/clarity, but I've been very careful not to affect the content and meaning of his answers.

1. How did you get access to the software you tested? Were they all free downloads?

Unfortunately not all are free to download, but with a certain effort it was possible to find them, although sometimes retrieving the latest patch is really impossible.

2. What experience did you have in SCADA / control systems prior to this effort?

Absolutely zero. I have never used the products I tested, and the situation has not changed much after the tests. I didn't go deeper into the software that I tested, after all it was just an experiment.

Dale's Interview with Luigi

"Anyway I have some other SCADA vulnerabilities in my pocket and 3 of them are about a very big vendor, but at the moment I have still not planned the releasing of these additional security bugs or if they will be under full or responsible disclosure."

- ICS-CERT reached out to Luigi to inquire about his claims
- Luigi disclosed the vendor name, but no other details
- ICS-CERT notified the vendor who contacted Luigi Auriemma
- Luigi asked the vendor for compensation for his research work
- The vendor declined
- No further communication has occurred between Luigi and the vendor

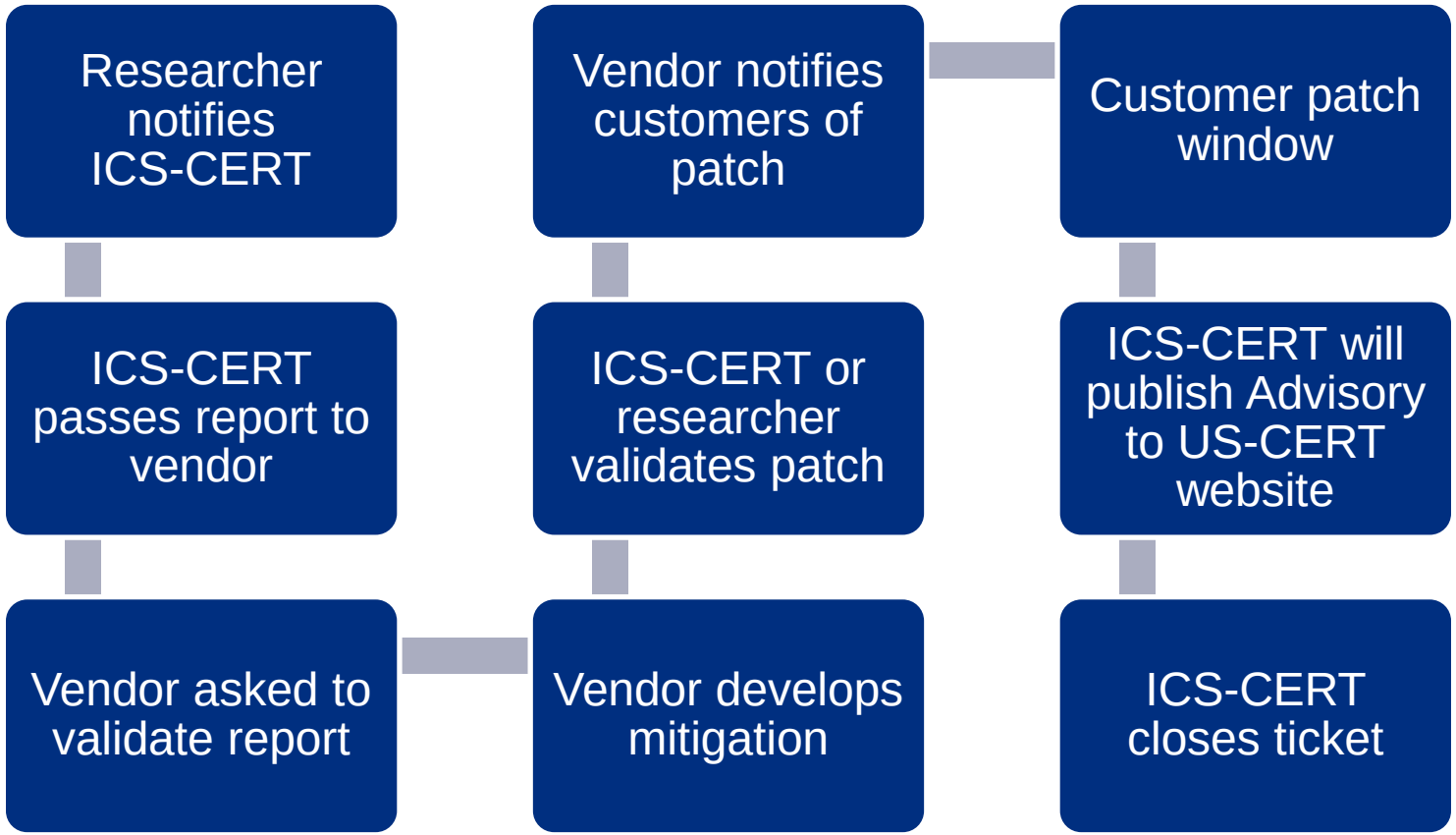
ICS-CERT Vulnerability Coordination

- Coordinated Vulnerability Disclosure (Responsible Disclosure)
- Unanticipated Vulnerability Disclosure (Full Disclosure)

Coordinated Vulnerability Disclosure

- Reporter contacts the vendor, ICS-CERT, or other coordination organization prior to public disclosure of vulnerability details
- ICS-CERT provides attribution to reporter in all ICS-CERT products

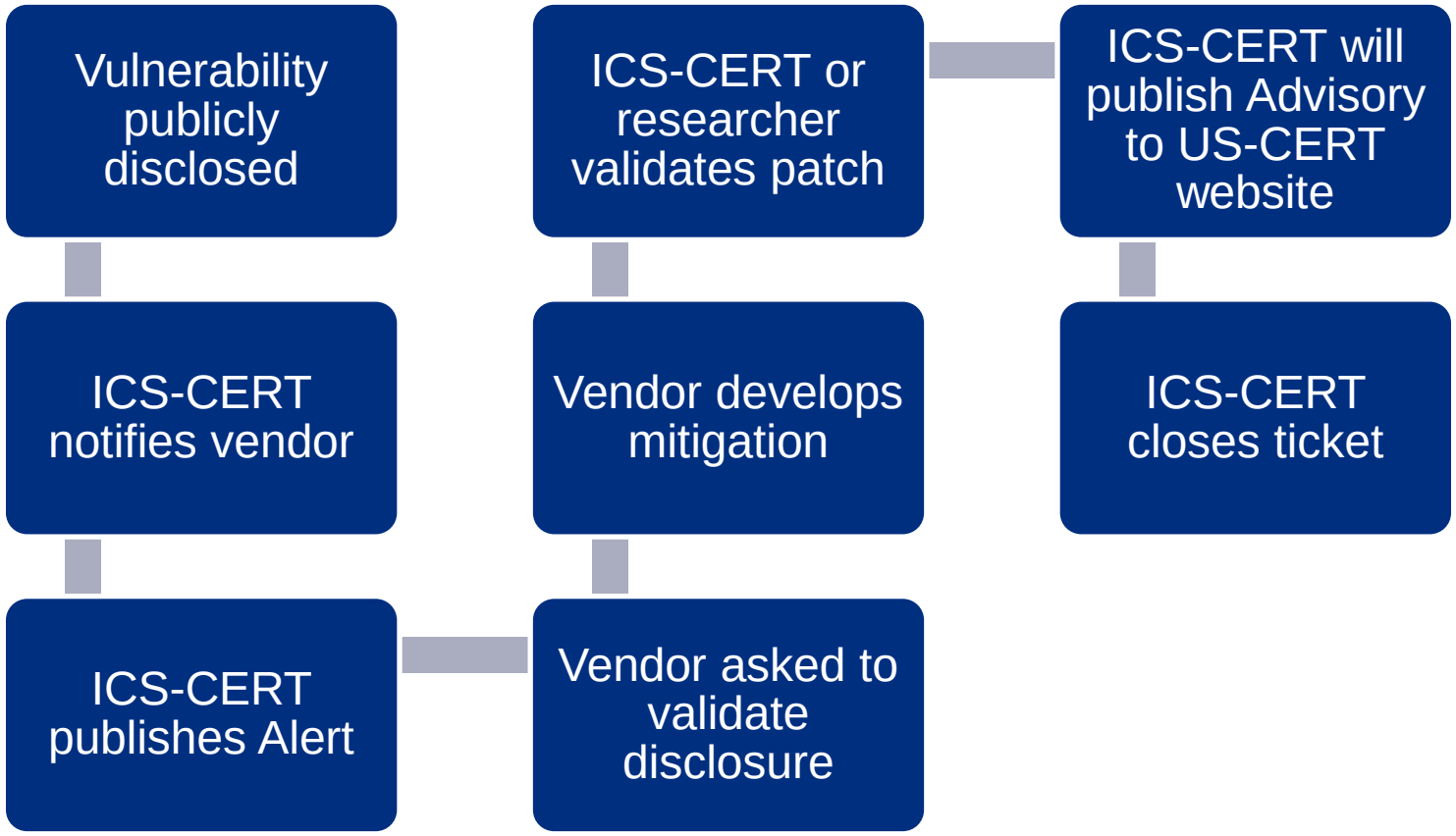
ICS-CERT Coordinated Vulnerability



Unanticipated Vulnerability Disclosure

- Reporter publicly discloses vulnerability details without contacting the vendor, ICS-CERT, or other coordination organizations
- ICS-CERT does not provide attribution to reporter in published products

ICS-CERT Unanticipated Vulnerability



Homeland Security