FBI Equity Discussion
April 24, 2014

Use of Zero-Days & Policy

Commercial & Government Information Technology and Industrial Control Product or System
Vulnerability Equity Policy & Process
0-day

- Concerns to consider

- CID will
Vulnerability Equity Policy & Process

- Mandate: Implement the policy to disseminate information about hardware and software vulnerabilities known to the USG found in GOTS, COTS or other commercial IT or industry control products or systems.

- Purpose: To ensure that dissemination decisions regarding the existence of a vulnerability are made quickly, in full consultation with all concerned USG organizations and in the best interest of the USG mission of cybersecurity, information assurance, intelligence, counterintelligence, law enforcement, military operations and critical infrastructure protection.
Process Overview: When a Vulnerability is Identified

- 1st classify or designate for special handling
- Determine if the vulnerability reaches the threshold. If so, notify the Executive Secretariat* (ES) ASAP.
  - Criteria - the vulnerability must be both newly discovered and not publicly known
  - Optional - vulnerabilities identified prior to the effective date of April 7th.
- The ES will notify all VEP POCs of the vulnerability and request they respond if they have an equity at stake and want to participate in the decision process.
- SME from each organization with an equity will participate in the discussions to produce recommendation to the ERB for decision

*The NSA/Information Assurance Directorate will serve the Executive Secretariat
The policy document "Commercial and Government Information Technology and Industrial Control Product or System Vulnerability Policy and Process" dated 2/16/10 was provide by email.

Point of contact on policy matters for the FBI is Cyber Division, Strategic Initiatives UC
The focus of this committee is to ensure dissemination decisions regarding the existence of a vulnerability is made quickly, in full consultation with all concerned divisions and in the best interest of intelligence collection, investigative matters and information assurance. Understanding that in most circumstances all three interest will not be satisfied but the best resolution for the overall good will be put forth to the USIC ERB.
FOR OTD INTERNAL USE

All,

I will be going on annual leave and will not be able to participate in the meeting on 4/21. I have pulled together some of the more relevant points to help OTD discuss and gather a position on this matter. I will be available later today to discuss in detail if there are any questions. Until OTD management establishes a position, I ask that further distribution of this message be limited.

[Name] has spoken to [Name]. He and his SC have been invited to represent CID at the meeting on Monday.

Thanks,
Sent: Thursday, April 24, 2014 9:57 AM
Subject: RE: Vulnerability/Zero-day discussion --- SECRET [(U)]

Classification: SECRET

Classified By: C37W35B81
Derived From: FBI NSIC, dated 20120629
Declassify On: 20391231

-------- TRANSITORY RECORD --------

V/R

SSA
Major Case Coordination Unit
FBIHQ/CID
Office
Cell:
-----Original Appointment-----

From: (OTD) (CON) On Behalf Of (OTD) (FBI)
Sent: Wednesday, April 23, 2014 12:37 PM
To: CD (FBI); (FBI); Cyd (FBI); (DO) (FBI);
(CYD) (FBI); CTD(FBI); (OTD) (FBI);
(OTD) (FBI)
Subject: Vulnerability/Zero-day discussion --- SECRET
When: Monday, May 05, 2014 10:00 AM-12:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: HQ Rm11160

Classification: SECRET

 Classified By: F23M23K53
 Derived From: FBI NSIC, dated 20120629
 Declassify On: 20391231

Hello,

Thank you in advance for your assistance;