Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Proposal for Managing System Security Patches in an Enterprise Network

Managing the security of a large complex enterprise network is a difficult and daunting task. Critical business needs rely on numerous types of operating systems running various applications that are inherently not secure. New vulnerabilities in various applications and operating systems are found every day. The rapid increase to guard against known vulnerabilities being released shows an essential need to implement an enterprise-wide process. This paper details one means of tracking the multitude of serious vulnerabil...

Copyright SANS Institute

Author Retains Full Rights

AD

**Proposal for Managing System Security Patches in an Enterprise Network**
Karenda Bernal
January 30, 2002

## 1.0 INTRODUCTION

Managing the security of a large complex enterprise network is a difficult and daunting task. Critical business needs rely on numerous types of operating systems running various applications that are inherently not secure. In an average week from January 10th, 2002 to January 16th, 2002 the vulnerability tracking website SecurityTracker (http://www.securitytracker.com) listed 60 new vulnerabilities in various applications and operating systems, for the same period BugTraq at Security Focus (http://www.securityfocus.com/cgi-bin/archive.pl?id=1&threads=0&start=2002-01-10&end=2002-01-16) listed 97 new vulnerabilities. The rapid increase to guard against known vulnerabilities being released shows an essential need to implement an enterprise-wide process. This paper details one means of tracking the multitude of serious vulnerabilities that affect our fictitious large-scale enterprise network and require us to implement patches. The paper does not detail the difficulties that ensue when trying to determine what effect the patches may have on business applications, only how to manage the implementation of patches across the enterprise with a large yet busy staff of Information Technology (IT) and security professionals. This paper details one possible solution to establishing an Emergency Vulnerability Alert (EVA) structure, the EVA process preparation; what will need to be in place prior to the implementation of the process, a complete layout of the EVA process detail, and finally what challenges (downfalls) may be faced with implementing the process proposed in this practical.

This process of managing security patches is only a small part of the overall security methodology used to protect an organization's assets. To learn more about a complete process this author suggests that you start with the Carnegie Mellon University's Software Engineering Institute Computer Emergency Response Teams webpage (http://www.cert.org/security-improvement/skip.html), there you will find the 'Security Knowledge in Practice', a step by step module assisting you with complete steps to securing an enterprise. Refer to Figure 1.0.

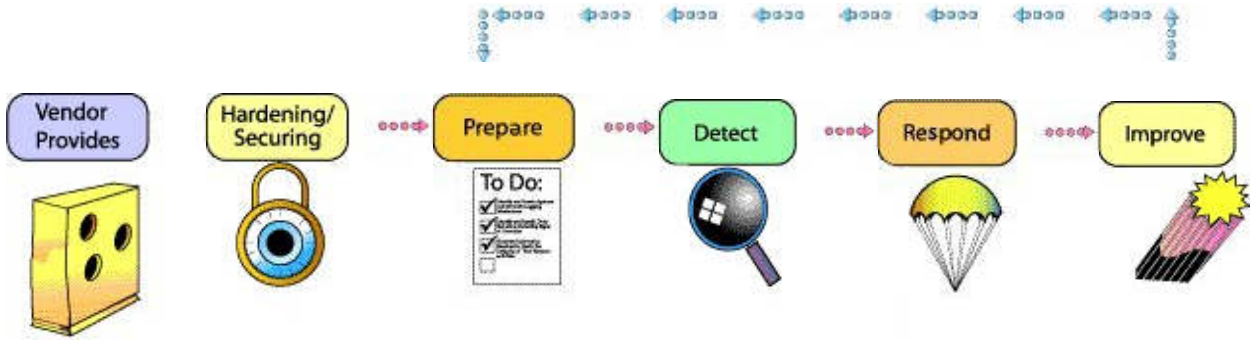


Figure 1.0 – Security Knowledge in Practice (Figure contains embedded links)

## 2.0 EVA STRUCTURE

The layout of the enterprise EVA structure may vary depending on the business type of the enterprise, the types of assets the enterprise owns, as well as the type of assets the enterprise may interface with, the number of personnel responsible for the network, and the geographical disbursement of the enterprise. One possible solution an enterprise may implement is depicted in Figure 2.0. The Emergency Security Response Team (ESRT) is the entity that collects all information about the vulnerabilities and the patches. They are responsible for being up-to-date on all new vulnerabilities being identified by vendors, outsourced contractors, web-site postings, hacker posting sites and various other sources. Once the vulnerability has been identified the ESRT communicates with the responsible vendors to obtain patches and solutions. The ESRT notifies and provides patches and solutions to the Computer Security Office (CSO). The CSO is the focal point of the enterprise for all security related matters. The CSO is the decision point and approval authority for network security for the enterprise. In order for the CSO to make sound decisions the Vulnerability Assessment Team (VAT), Certification & Accreditation (C&A), and the Computer Incident Response Team (CIRT) all work together to support the CSO. These 3 groups provide essential information to the process concerning assets, policing the process for compliance, and responding to any incidents that may occur. The Security Assurance Managers (SAM) may be designated by geographic location of the assets for the enterprise. The SAMs are responsible for enforcing the security procedures, policies, and ensuring all subordinates have received training. In this case there are 3 different regions differentiating the SAMs: the enterprise backbone, the Seattle W.A. office, and the Washington D.C. office. The SAMs appoint Security Assurance Network Officers (SANO). The SANOs are responsible for all security network matters at that location. In the example there are 2 SANOs appointed for the Seattle W.A office and the Washington D.C. office: one for Unix assets and the other for Windows assets. Beneath the SANOs are the System Administrators (SA) divided into areas of responsibility (desktops and servers). The SAs are (Know thy System) responsible for configuration, maintenance, testing and application of the patches. Reporting to the SAM Backbone Devices is the SANO with appointed SA designated for Intrusion Detection Systems (IDS), Firewalls, and Routers. All participants in the EVA structure must acknowledge and report on all vulnerability alerts released from the CSO.

Figure 2.0 – EVA Structure

## 3.0 EVA PROCESS PREPARATION

An enterprise must prepare prior to any process implementation. The initial preparation will determine the success or failure of an effective EVA process. Keeping this in mind the preparation phrase will generally be the most time consuming activity for ensuring a successful process. The steps for the EVA process preparation are identified below:

- Establish policies/procedures
- Establish EVA structure (identify key personnel in the process)
- Identify assets in the enterprise. (*Note – this can initially be accomplished through information obtained from the Connection Approval Packages (CAP) or Certification/Accreditation Packages.)
- Select tools to automate process (tools to apply patches, tools to scan network for compliance, tools to manage the process and progress of patches)
- Establish training program
- Establish Security Awareness Program
- Identify a checklist to be followed for "Checks and Balances" to track compliance and overall process wellness

This list of steps for EVA process preparation is not inclusive and may need revision depending upon enterprise needs.

## 4.0 EVA PROCESS DETAILS

### 4.1 Vulnerability Discovered

*Description:* The process of discovering that a vulnerability exists.

*Activity Steps:* Receiving information from a source.

*Business Rules:*

- Discovery of vulnerabilities may come from several different sources including responsible vendors, postings on the web (information bulletin sites or hacker websites), outside organizations, internal agencies, newspapers, or media.
- Organizations will outsource to an outside agency that dedicates time and resources to researching and keeping abreast of current events relating to network security.
- Sources must be validated by the Chief, Emergency Security Response Team (ESRT) or a designated representative.

### 4.2 Validation of Vulnerability with Affected Vendor

*Description:* The process of checking with the affected vendor for validity of vulnerability identified.

*Activity Steps:* Contact affected vendor via email with follow-up telephone call

*Business Rules:*

- Telephone call will be conducted on a land line if information about vulnerability is determined to be a security risk to the enterprise.
- Information will be recorded via tracking log file for accountability i.e. date, time, individuals involved, individual at the vendor site that confirmed information, any information received from the vendor i.e. patches or solutions.

### 4.3 Generate EVA message

*Description:* The process of ESRT generating an EVA message

*Activity Steps:* Type an email message with description of vulnerability, known assets affected, recommended solutions and links to

patches

*Business Rules:*

- There are 3 types of messages that may emanate from ESRT:
    - Emergency Vulnerability Alert – requires acknowledgement and reporting action
    - Emergency Vulnerability Bulletin - requires acknowledgement but does not require reporting
    - Emergency Vulnerability Tech Tip – gets distributed to all (Security Assurance Manager) SAMs/SAs but does not require acknowledgement or reporting.

**4.4 Distribute EVA message to CSO**

*Description:* The process of distributing the EVA message to the Chief Security Office (CSO).

*Activity Steps:* Send email message to CSO

*Business Rules:*

- ESRT will have 24 hours to generate and draft email message

**4.5 CSO receive message**

*Description:* The process of receiving the email message from ESRT

*Activity Steps:* Receive email

*Business Rules:*

- Email will be monitored 24 * 7.
- During non-business hours this email traffic will be monitored by the helpdesk at a minimum hourly. If an alert is released, helpdesk will contact primary or secondary CSO contact.

**4.6 CSO conducts comparison of EVA with Asset Management System (AMS)/Configuration Management System (CMS)**

*Description:* Comparison of EVA with assets owned in enterprise

*Activity Steps:* Review assets affected in the EVA, query the AMS and CMS to identify if the enterprise owns any of the asset types identified in the EVA

*Business Rules:*

- The AMS and CMS must be updated within 24 hours of actual network change for accountability.

**4.7 CSO reviews Enterprise Security Manager (ESM)**

*Description:* Review of ESM logs

*Activity Steps:* Review ESM logs to see if vulnerability has been exploited within the enterprise.

*Business Rules:*

- ESM will obtain log files from firewalls, IDS, routers, syslog servers, critical servers, and other network addressable devices.
- If vulnerability is discovered in the enterprise the CSO will follow Emergency Incident Handling Procedures
- If no assets match per log then skip this step

**4.8 Acknowledge receipt in ESRT Information Assurance (EIA) database**

*Description:* The process of the CSO entering the EIA database indicating receipt and preliminary status of the EVA.

*Activity Steps:* Log into the EIA database and complete the EVA checklist

*Business Rules:*

- Mandatory Fields must be completed on the EVA checklist (Date/Time Acknowledge Receipt of EVA, Preliminary status of affected systems, Preliminary status of possible exploited systems, SAM and SA suspense dates)

- Must complete EVA checklist within 5 days unless otherwise specified by ESRT.

**4.9 Distribute to SAM**

*Description:* The process of distributing the message to the appropriate SAM.

*Activity Steps:* Create an email message, highlight what the EVA is, what assets are affected, information acquired from the comparison of the AMS/CMS and ESM, required action to fix, and a suspense date to the CSO

*Business Rules:*

- Email will be distributed to appropriate SAM responsible for the assets affected by the EVA.
- A Courtesy Copy will be distributed to all SAMs, SANOs, and SAs in the enterprise to reduce the risk of any assets that were not updated in the AMS and CMS.
- All EVA messages must be acknowledged prior to entering reporting status.

**4.10 SAMs and SAs receive message**

*Description:* SAMs, SANOs, and SAs receive email message

*Activity Steps:* Receive email

*Business Rules:*

- During non-business hours the CSO will maintain an emergency contact list of all SAMs, SANOs, and SAs within the enterprise for immediate contact in case of a possible breach in the security of the enterprise.

**4.11 Acknowledge receipt in EIA database**

*Description:* The process of the SAMs, SANOs, and the SAs entering the EIA database and indicating receipt and preliminary status of the EVA.

*Activity Steps:* Log into the EIA database, Acknowledge receipt of EVA and Update EVA checklist

*Business Rules:*

- Mandatory Fields must be completed on the EVA checklist (Date/Time Acknowledge Receipt of EVA, Preliminary status of affected systems, Preliminary status of possible exploited systems)
- Each SAM, SANO, and SA will only be able to preview and update information on assets that they are responsible for.
- Each SAM must account for all SANOs in their chain. The SANOs must account for all SAs in their chain. The SANO report will be a roll-up of all the SAs. The SAM report will be a roll-up of all the SANOs.
- If a SAM, SANO, or SA determines that there has been an asset that was not identified in the initial identification process, they will contact the CSO via email with follow-up telephone call.

- Must acknowledge, update EVA checklist, and if applicable contact the CSO with any assets that were not initially identified within 5 days unless otherwise specified by CSO.

**4.12 EIA database receives input and generates initial report for the Chief Security Officer's Review**

*Description:* The process of the EIA receiving inputs, querying database, and automatically generating a report for the CSO for review.

*Activity Steps:* Once database conditions are met (Receipt of input from all the SAMs/SANOs/SAs or flag triggered from the suspense

date that was input into the database from the CSO) A query is performed and the initial report is automatically generated.

*Business Rules:*

- If CSO changes any suspense dates they must notify all SAMs, SANOs, and SAs to ensure all updates are completed prior to report running.
- The report will also indicate any SAMs, SANOs or SAs that are delinquent/negligent

**4.13 SAM conducts research on EVA and possible assets affected.**

*Description:* The process of comparing the EVA with assets to determine if it affects assets

*Activity Steps:* Compare the EVA with assets to determine if it affects assets

*Business Rules:*

- Suspense date will be established by the CSO, this will be determined by the severity of the EVA.

**4.14 SAM coordinates with appropriate SANO and SA**

*Description:* The process of SAM coordinating with SANO and SA

*Activity Steps:* SAM provides details of information discovered from research conducted.

*Business Rules:*

- If SAM research has indicated that there are no assets affected, this step will still be followed to ensure nothing has been added to the network that they are unaware of.
- SAM may be responsible for several SANOs within a specified portion of the enterprise. The SANOs may be responsible for several SAs within a specified portion of the enterprise. It is the responsibility of the SAM to ensure all reporting is completed.
- SANOs and SAs are required to have extensive security technical training in accordance with enterprise policy.

**4.15 SANO and appropriate SA reviews information and conducts in-depth analysis of data and configuration of affected assets.**

*Description:* The process of the SANO and the appropriate SA analyzing data received from the SAM and checking complete configuration of system.

*Activity Steps:* Analyze EVA, data provided from the SAM, patch information, configuration of system.

*Business Rules:*

- Information will be documented and logged for traceability.
- If it has been determined that EVA does not affect SANO, this step will not be applicable.

**4.16 SANO provides analysis outcome to SAM**

*Description:* The process of the SANO coordinating with the SAM to provide information discovered from in-depth analysis

*Activity Steps:* The SANO will provide log to the SAM and discuss any concerns with the EVA itself.

Business Rules:

- During this coordination with the SAM, it will also be determined if the asset can be fixed prior to the suspense date that the CSO has indicated or if waiver is required to EVA.
- If it has been determined that EVA does not affect SANO, this step will not be applicable.

**4.17 Complete request for extension/exemption**

*Description:* The process of requesting an extension/exemption.

*Activity Steps:* Complete extension request form

*Business Rules:*

- An organization may need to request an exemption if it is found that an EVA may be incompatible with specific applications.
- Must request an extension NLT 3-5 business days prior to the EVA suspense date.

**4.17.1 Forward request with copy of EVA to CSO**

*Description:* The process of submitting an extension/exemption request to the CSO.

*Activity Steps:* Email the extension/exemption request and a copy of the EVA.

*Business Rules:*

- This request is to be submitted and responded to (granted or not) prior to the suspense date indicated on the EVA

**4.17.2 CSO reviews request and determines approval / disapproval status**

*Description:* The process of reviewing extension/exemption request to determine if the extension should be approved/disapproved.

*Activity Steps:* The CSO will review request, gather information if required to assist the Chief Security Officer in making decision of approval/disapproval.

*Business Rules:*

- If decision requires technical support the request will be reviewed by a designated team consisting of a member from the following areas: CSO, C&A, VAT, Security Engineering Staff, CIRT and Network Staff

**4.17.3 Notify requesting organization's SAM of approval / disapproval status**

*Description:* The process of notifying the SAM of the CSO's decision to approve/disapprove extension/exemption.

*Activity Steps:* Contact the SAM via telephone

*Business Rules:*

- Decision for approval/disapproval must be made prior to EVA suspense date.

**4.17.4 Enter approval / disapproval into IA database**

*Description:* The process of entering the IA database and inputting approval/disapproval status.

*Activity Steps:* CSO updates the EIA database to reflect approval/disapproval of extension.

*Business Rules:*

- If the Chief Security Officer disapproves extension/exemption request an explanation will be annotated in the EIA database.

**4.18 Fix Assets**

*Description*: The process of the SA applying the fix as indicated by the EVA

*Activity Steps:* SA will Fix Assets

*Business Rules:*

- Must apply the fix action by suspense date as indicated in the EVA message
- SAs are required to test the configuration and patches before placing on production systems.

ESRT cannot verify EVERY installation or configuration currently in use.

**4.19 Report # of fixed assets into EIA database**

*Description:* The process of entering the EIA database and indicating the number of fixed assets.

*Activity Steps:* The SA will report # of fixed assets in the EIA database, the responsible SANO will rollup all the SAs reports, validate the # of fixed assets, and report to the responsible SAM. The SAM will rollup all the SANOs reports, validate the # of fixed assets, and report to the CSO.

*Business Rules:*

- Suspense date to the IAO will be at least 2 days prior to suspense date in EVA Message, this allows time for the IAO to do the validation and rollup for the entire organization.

**4.20 CSO reviews # of fixed assets from the entire enterprise**

*Description:* CSO review of EVA reporting

*Activity Steps*: CSO will review # of assets reported by each SAM within the enterprise and compile a status report

*Business Rules:*

- CSO must do a comparison between initial report and final report from the SAMs.
- If any discrepancies are discovered the CSO will contact the SAM to resolve.

**4.21 Scan network**

*Description:* The process of scanning network for compliance with EVA.

*Activity Steps:* CSO will provide list to VAT to scan for compliance with EVA.

*Business Rules:*

- The scan will use appropriate scan tools to scan for the specific vulnerability identified in the issued EVA.
- VAT will give SAM courtesy call prior to scan but no pre-authorization is required
- Scans will not be done to every network, every EVA, only a sampling of each EVA for compliance.

**4.21.1 Analyze network scan results**

*Description:* The process of VAT reviewing results of network scan to identify any systems that have not applied the fix action.

Activity Steps: VAT will analyze data from network scan and report any suspicious results to CSO.

*Business Rules:*

- VAT must notify CSO immediately if an asset that was reported compliant is scanned and found to be non-compliant, or if any other anomaly is detected.

**4.22.2 Log network scan**

*Description:* The process of logging the results of the network scan in the EIA database.

*Activity Steps:* VAT will annotate the results of the scan in the EIA database for the CSO review.

*Business Rules:*

- Results must be logged within 48 hours after scan has been completed.

**4.23 Determine if fix is valid**

*Description:* The process of differentiating between valid fixes and invalid fixes via the scan.

*Activity Steps:* CSO will do a comparison between scan results and # of assets reported from the SAM.

*Business Rules:*

- CSO will contact the SAM immediately if there is a discrepancy between the # of assets reported compliant and the VAT scan results.

**4.24 Validation of fixed assets in database**

*Description:* The process of the CSO validating the assets reported by subordinate units.

*Activity Steps:* CSO will report all verified assets through the EIA database to the ESRT.

*Business Rules:*

- CSO must validate all assets prior to the suspense date for reporting to the ESRT.

**4.25 CSO reports to ESRT**

*Description:* The process of the CSO reporting all compiled information to the ESRT.

*Activity Steps:* CSO compiles all information reported from all SAMs and generates final report to ESRT.

*Business Rules:*

- CSO must notify ESRT of any systems that have extensions or exemptions granted.

**5.0 CHALLENGES (DOWNFALLS)**

There are several challenges or downfalls in managing system security patches in an Enterprise Network that must be recognized and addressed. An excerpt from the article "Feds take minimal role in patching holes in cyberspace" written by Neil Munro, National Journal refers to the writing of the Prussian strategist Carl von Clausewitz in the early 1800s. Clausewitz wrote that even the simplest things are difficult to accomplish during war. A statement that still holds extreme validity. The process above that has been laid out seems simple and straightforward. Don't let the words written in this practical lead one to believe as long as the process is documented and implemented accordingly, down to each step being followed and accounted for that there are no hurdles to cross. Security professionals are faced with challenges every day. Nothing remains static. With a firm understanding things change rapidly and complete tranquility is impractical this section will cover several challenges and downfalls that may play a factor in managing system security patches. It will shed light on the difficulty of managing system security patches and confirm that the statement written several decades ago still remains true. The challenges and downfalls that will be discussed include management non-acceptance, vulnerable system and software releases, untrained personnel, incomplete testing of patches, time constraints, and geographically dispersed networks.

The first and biggest hurdle to get over is having management understand and accept that this is an essential process that must be implemented in order to secure the enterprise. This would seem to be intuitive and should not have to be discussed as a challenge or downfall due to statistical data indicated in the Introduction of this practical. What may seem to be common sense to security professionals across the board may be viewed as a burdensome task from the management standpoint. One question that will be posed from management is "How much will it cost?". Inevitably nothing is free but the phrase "Pay me now, or pay me later" is the real question to be answered. On February 23, 2000 Dr. Vinton G. Cerf, Senior Vice President of Internet Architecture & Technology MCI WorldCom testified in front of the Senate Joint Economic Committee. Dr. Cerf referenced a survey conducted by the Computer Security Institute (CSI) "62 percent of companies have experienced computer breaches; 51 percent of respondents reported financial losses due to computer security problems; criminal hacking losses of the 163 responding organizations was placed at $123 million in 1998 and is climbing at an extraordinary pace. The Institute found that system penetration by outsiders has risen in each of the past three years as has unauthorized access by insiders. Twenty-six percent of respondents in the CSI study reported theft of proprietary information and 27 percent reported financial fraud. Twenty percent reported unauthorized use or misuse of websites. Virus episodes like Melissa and Chernobyl are becoming more frequent. The Symantec Anti-Virus Research Center estimates that new viruses are being launched at a rate of 10 to 15 per day and that over 2400 currently exist. Thirty-five percent are considered to be intentionally destructive." http://www1.worldcom.com/global/resources/cerfs_up/issues/testimony.xml

The 2001 Computer Security Institute/FBI Computer Crime Survey quoted "thirty-five percent of respondents (which equated to 186 respondents) willing to quantify their financial losses, they reported $377,828,700 in losses. In contrast, the losses from 249 respondents in 2000 totaled only $265,589,940. The average annual total over the three previous years prior to 2000 was $120,240,180." Will management be willing to spend the time, money, and resources required to implement this process, or wait until their network is rendered inoperable?

Equally important to note is the downfall which comes from vulnerable system and software releases. The releases have not been secured and thoroughly tested. The market is driving vendors to release new and or upgraded versions that have not had the time to go through rigorous testing. Vendors want to make money and the people want the products. It is almost impossible to account for every possible security hole that may exist. Therefore; in general most products are set at minimal security requirements or non-existent ones when received by the consumer. This is not to state that vendors are intentionally trying to harm or mislead the consumer they just simply do not have the time. But the focus seems to be taking a turn. Microsoft Bill Gates in an email 17 January 2002 http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanA%2edb&command=viewone&id=49 had stated "When we face a choice between adding features and resolving security issues, we need to choose security," "Our products should emphasize security right out of the box and we must constantly refine and improve that security as threats evolve.

The next challenge is ensuring everyone involved in the program is adequately trained. Stephen Northcutt head of the System Administration, Networking, and Security (SANS) Institute's Global Incident Analysis Center identified to the public the extent of damage that untrained individuals were causing. Northcutt and a team of security professionals formed a working group that identified a set of minimum necessary skills required for security professionals. This minimum necessary skills identified is known as "security essentials." A checklist was constructed from this working group to help management be able to identify the skill set of their IT staff securing the networks. Security training is available from various organizations with multiple locations. A couple reputable organizations include the SANS Institute http://www.sans.org/newlook/home.php and the Carnegie Mellon Software Engineering Institute http://www.cert.org/nav/index_gold.html Informative information obtained from the web-page "The CERT®/CC is collaborating with the Carnegie Mellon University H. J. Heinz III School of Public Policy and Management to develop a curriculum in information security management. CERT/CC staff members are teaching courses in the Information Security Management specialization of the Master of Information Systems Management program." There are tools to help identify any deficiencies within the IT staff and if found there are numerous courses and conferences in which they may attend to expand their knowledge.

Yet another downfall is incomplete testing of the patches that are released. The task of keeping systems operational yet secure becomes even more difficult when new patches are released for newly published vulnerabilities that are not tested thoroughly with all applications. Sometimes a dangerous vulnerability exist that requires a patch from the vendor to keep malicious minded individuals from taking over a system, however when the patch is applied it may make adversely affect the system or worse yet crash the box completely. A recent example that comes to mind is the Microsoft Windows NT 4.0 Security Roll-Up package. When users installed this package that were using the Compaq Smart Array Controller (multiple versions, see http://support.microsoft.com/default.aspx?scid=kb;EN-US;q305228 for details) they received an error message on Windows wonderful ‘Blue Screen of Death’. There are generally work-arounds when receiving something like this as this case shows, however imagine dealing with problems like this and trying to keep up with the standard system administrator duties as well.

The last two items that need to be accounted for are time constraint issues as well as geographically dispersed networks. The first issue of time constraints is one that has been hard to grapple. Generally patches and hot-fixes have come out quite frequently as we discussed earlier in this paper. SA are already overburdened with the day-to-day operations of a network requiring new systems to brought online, upgrades to be completed, systems to be repaired, backups to be completed, software to be loaded, and reports to be written to name a few. Many feel that they do not have adequate time to install important patches, others are not kept informed of the latest security patches and therefore do not know to install them. Along that line there are also millions of home users that have computers that either do not know of the latest patches needed to secure their system or are afraid installing it might 'break' their system. Geographically dispersed networks are difficult to manage, having a staff capable of handling all IT functions at each site is sometimes not cost effective. Flying your staff around to install patches and manage systems might not be the most cost effective means either. Luckily there are new products on the market and existing products that are being upgraded that can help. SMS can be used in a limited fashion, Blade Logic has some exciting new technology allowing complete remote management of software from a distance. Technology might be the means to solve this technology issue.

**6.0 SUMMARY**

When trying to grasp how to implement even the simplest of tasks in IT that effort can become extremely challenging. Managing System Security Patches in an Enterprise Network is not a menial task. This practical is merely a proposal for a solution to this complicated process. Vulnerabilities and their related exploits continue to rise at an exponential rate. The Presidential Decision Directive (PDD) 63 has directed corporate America and federal government to take this matter seriously and secure their networks. Statistics prove it is in the benefit of an enterprise to take the time to ensure a process is in place to patch their systems when vulnerabilities are identified and patches are released. This paper has designed an EVA structure to present one means of formulating a process for an organization’s practical implementation of security patches.

Utilizing this process can give reasonable assurance of safety and security for an enterprise network. The challenges (downfalls) highlighted at the conclusion of the practical are by no means insurmountable and must be taken into consideration as the process evolves.

**ACRONYMS**

**AMS** – Asset Management System

**C&A** – Certification & Accreditation

**CIRT** – Computer Incident Response Team

**CMS** – Configuration Management System

**CSI** – Computer Security Institute

**CSO** – Computer Security Office

**ESM** – Enterprise Security Manager

**IA** – Information Assurance

**IDS** – Intrusion Detection System

**IRT** - Incident Response Team

**IT** – Information Technology

**EIA** – ESRT Information Assurance

**ESRT** – Emergency Security Response Team

**EVA** – Emergency Vulnerability Alert

**SA** – System Administrator

**SAM** – Security Assurance Manager

**SANO** – Security Assurance Network Officer

**SANS** - System Administration, Networking, and Security

**VAT** – Vulnerability Assessment Team

**REFERENCES**

1. Carnegie Mellon University's Software Engineering Institute Computer Emergency Response Teams web-page (Security Practices & Evaluations) http://www.cert.org/security-improvement/skip.html

2. Carnegie Mellon University's Software Engineering Institute Computer Emergency Response Teams web-page (Training and Education) http://www.cert.org/nav/index_gold.html

3. Computer Security Institute (CSI), Computer Security Issues and Trends, VOL. VII, NO. 1 Spring 2001, 2001 CSI/FBI Computer Crime and Security Survey, Richard Power, Editorial Director, CSI

4. COMPUTERWORLD, A security skills test, Alan Paller, 17 July 2001, http://www.computerworld.com/cwi/story/0,1199,NAV65-663_STO47140,00.html?s

5. CBS MARKETWATCH, Computer security in spotlight, Allen Wan, 17 Jan 2002 CBS.MarketWatch.com http://www.marketwatch.com/news/yhoo/story.asp?source=blq/yhoo&siteid=yhoo&dist=yhoo&guid=%7B4BD19F77%2DBA53%2D4AA7%2D91E2%2D00542F2BD378%7D

6. Microsoft Product Support Services, "STOP 0xA" Occurs After Applying Windows NT 4.0 Security Rollup Package (Q305228), Published: Aug 8, 2001 3:41A.M.

Last Modified: Oct 11, 2001 3:25 P.M. http://support.microsoft.com/default.aspx?scid=kb;EN-US;q305228

7. GovExec.com "Feds take minimal role in patching holes in cyberspace", Neil Munro, National Journal, January 4, 2002
http://www.govexec.com/

8. SANS Institute, http://www.sans.org/newlook/home.php

9. Security Focus, Bugtraq Archive, Message Index from 2002-01-10 to 2002-01-16
http://www.securitytracker.com/

10. Security News Portal (SNP), Complete text of the Bill Gates "Trustworthy Computing" Memo, 01-17-2002 -- Memo from Bill Gates
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanA%2edb&command=viewone&id=49

11. Security Tracker http://www.securitytracker.com/

12. Social, Economic and Regulatory Issues, Statement of Dr. Vinton G. Cerf, Senior Vice President of Internet Architecture & Technology MCI WorldCom Senate Joint Economic Committee, February 23, 2000
http://www1.worldcom.com/global/resources/cerfs_up/issues/testimony.xml

13. "The CERT Guide to System and Network Security Practices", Julia H. Allen, Copyright 2001 by Addison-Wesley

14. Protective Americas Critical Infrastructures Presidential Decision Directives (PDD) 63, The Whitehouse Washington, Former President William J. Clinton, May 22, 1998.

Last Updated: June 20th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Melbourne 2013** | **Melbourne, AU** | **Sep 02, 2013 - Sep 07, 2013** | **Live Event** |
| **SANS Capital City 2013** | **Washington, DCUS** | **Sep 03, 2013 - Sep 08, 2013** | **Live Event** |
| **Network Security 2013** | **Las Vegas, NVUS** | **Sep 14, 2013 - Sep 23, 2013** | **Live Event** |
| **SANS Canberra 2013** | **OnlineAU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |