Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)

Practical Assignment – Version 1.4b

By: Minh Tran
Submitted on: December 16, 2003

HP-UX Security Patch Management

CONTENTS

HP-UX Security Patch Management

Abstract

Steve Ulfelder in Network World, 10/21/2002 on “Practical Patch Management”, “Patch management quickly can flatten IT departments as they struggle to find the time and resources needed to get the problem under control. The cost implications are huge. Aberdeen Group estimates the tab for patch management for U.S. businesses at $2 billion per year.” [1]

In any organization, security patch management is an essential but time-consuming and exhaustive process for the system administrator. The System Administrator is constantly struggling with applying the latest security patches and at the same time trying to maintain the stability and availability of the systems. Most patches require prerequisites and dependencies that will affect not only the operating system but the applications as well.

The System Administrator needs to acquire a good patch management methodology. Creating a process to acquire, identify, select, download and implement new software patches, all the while maintaining version control and ease of patching multiple systems. The System Administrator must be on constant alert for new security vulnerabilities and patches via automated reports, industry news and emails from vendor sites.

According to Ellen Messmer in Network World, 07/28/03 on “Patch management burdens customers”, “When it comes to patch management, there's no one-size-fits-all approach to doing a job no one wants to do: update software for new features, or the more troubling task, fixing a security hole before a hacker or computer worm finds it”. [2]

Description of the Issue

The issue of patch management is a pressing one on all IT management. Currently there is no procedure or policy on security patch management for our environment. Patches are not applied in a timely fashion or not at all. There is no consistent method when patches are applied. This results in systems that have a different level of security vulnerability.

Currently we manually download patches, manually search for dependencies patches and create a separate depot for security patches.

We need to research, discuss, develop and implement a consistent Patch Management process. It should give the System Administrator control over applying patches. Decrease the time spent on maintaining production systems within our organization.

It must accurately identify the vulnerabilities of each system, recommend the latest patches, take into account all dependencies and prerequisites necessary to accurately apply the patches in a varied environment.

Our Investigation

Before HP-UX Security Patch Check was available, we relied on receiving the Security Bulletin periodically via email from HP to identify any new security patches that had just come out to fix security vulnerabilities for the HP servers. We then had to log into HP's website, www.itrc.hp.com, and search for those new patches one at a time. Each time, searching for dependencies and superceded patches manually. After gathering all the patches, with the patch IDs, we would create a list of current patches on our HP server and compare it against the new patch list. A script was then run to download the new patches using ftp to a temporary directory on the HP server. A new depot was created to hold the new patches and then they were applied to the HP server. The process of identifying new patches, dependencies and superseded patches is very time consuming. Due to the manual nature of the process you would increase your chances for making mistakes on identifying and downloading dependencies and superseded patches. The process was applied to each server independently. Keeping the patch level consistent across multiple HP servers is a very time consuming process for the system administrator.

We wanted to find a tool that would assist us in keeping the HP-UX systems security patch level current for our servers. It should automatically produce a list of all required patches, not just security related patches. Notify us of patches currently installed that have been superseded by other installed patches on our server. Provide the ability to manage the installation of patches. Since our environment is HP-UX, we did some research at our vendor's website, www.software.hp.com, to find a Patch Management tool that would work within our environment. HP now provides a tool to find missing security patches on each system called "Security Patch Check". Security Patch Check allows us to automate the process to save time.

HP's "Security Patch Check is a tool that analyzes the currency of a system with respect to security patches. It recommends patches for security vulnerabilities that have not been fixed by other patches currently on the system. Use of the Security Patch Check software tool can help efficiently improved system security, but does not guarantee system security." [3] This tool will automatically download

the Security Patch Check catalog, comparing a catalog of security-related patches to the patches on our system. It generates a report of recommended patches, a description of the patches, any special instructions, if the system will need to reboot or not and whether the patches have any patch dependencies.

Our Decision

We chose HP-UX Security Patch Check from our vendor because we can easily obtain/download the software and install it on our systems. There is no need for configuration and there is no cost in using this product. However, this would only serve for our purpose of patching security holes on our systems. It does not include patching of OS and applications that are not security related.

HP-UX Security Patch Check is a semi-automated tool, but it's not a complete solution because its sole purpose is Security patches for the OS but not for application patching. HP has changed its patch methodology to upgrading applications versus patching. For example, a security vulnerable was found in HP-UX Secure Shell (SSH) but HP did not send out a notification concerning the security vulnerability. Instead we had to rely on other sources; i.e., being a member of other security alert groups, or searching through other websites, to learn of the problem. HP did not create a patch for that particular SSH security vulnerability, but instead release a new version of Secure Shell SSH. By applying security patches to the system, we don't know about the potential security holes for the applications. But for now, we will have to implement Security Patch Check tool to prevent security vulnerabilities on our systems.

Features and benefits

- Creates a report of recommended security patches to be installed.
- Automates checking for security patches not installed a system.
- Notifies the users if there are issues with any currently installed patches that are present on the system being analyzed.

Drawbacks

- Only provides patches on Security vulnerabilities.
- No patches for OS and applications as a whole.
- Applications are not being patched, only upgraded.
- Still have to manually download and install patches.

HP-UX Security Patch Check can be down load from vendor's website, www.software.hp.com. It also requires that Perl 5.005 or newer be installed on your system before security_patch_check can be run. No further configuration of the product is required. You can automate the reporting by placing security patch check in cron. This will allow you to schedule your reports and email the results to the appropriate people.

After running Security Patch Check a report is generated that will tell you whether any patches are recommended. The report includes any special information about the patch, whether a system reboot is required, if patch dependencies are needed and a description of the patch. Patch dependencies indicate whether the new patch is dependant on other patches before it is installed. This is set up as a scheduled job on our systems to receive this report once a week. Refer to Appendix A for the sample generated by running security_patch_check –r.

The report will also notify you with warnings if patches have a dependency conflict, if superceded patches are currently active or if they have been recalled. A superseded patch installed but not active on the system can become active if the superseding patch is removed. This can cause severe issues on a server and could result in extended downtime. All superseded patches should be removed once the new patches have gone through sufficient burn-in time. A recalled patch means the patch is known to produce other security risks on the system. HP will usually recommend another patch to be installed. Dependency conflict means the selected patch requires another patch to be installed with it.

"There are 4 types of security patch identification, an HP-UX patch name consists of a four-character type identifier followed by an underscore followed by a four or five digit number field. The numeric field, called the patch number, is unique for a patch regardless of patch type. The current defined patch types are:" [4]

PHCO – Commands and Libraries
PHKL – Kernel
PHNE – Networking
PHSS – All other HP-UX subsystems

Once the security patches that need to be applied have been identified, you can login with a user account and password to the vendor's website at www.itrc.hp.com. Using the patch database to search for and acquire those individual security patches. For each patch you can find the description, superseded patches, special installation instructions, dependencies etc. The patch description gives you information about the issue is being addressed. The superseded patch list will provide you a history of patches applied and provides you with the ability to select previous patches if the newly released patch may cause you problems. Special installation instructions are steps that you might

need to perform before or after the patch is installed. For example, modification of configuration files may be necessary or the installation of new library patches that an application is currently running which are still linked to the old version of the Library. Then a system reboot is necessary to re-link the applications so it will work properly with the newly installed library patches.

The list of patches is broken into 3 HP rating categories, “Specified”, “Recommended” and “Most Recent”. “Specified” is the patch that you entered in the search window. The “Recommended” patch is one that has been available for a sufficient time to prove it is reliable and did not introduce other problems. “Most Recent” is the newest and latest patch available and may supersede the “Recommended” patch.

In addition to the categories, each patch has a HP patch-rating from “★”, “★★” or “★★★”. “★★★" being the highest rating.

hp rating†	description
★	Patch has undergone functional testing by HP to verify that the patch fixes the problem that it purports to fix. No unwanted side effects were discovered. Also, HP has verified that the patch will install and de-install in its target environments.
★★	Patch has been installed in a certain number of customer environments with no problems reported.
★★★	Patch has been stress- and performance-tested by HP in simulated customer mission-critical environments using common application stacks. Not all patches undergo this testing.
	Patch contains warnings

†Table 1: Taken from
http://www1.itrc.hp.com/service/patch/wrap.do?pageKey=patch.html.patchDBCandidateListHelp&BC=patch.breadcrumb.main|patch.breadcrumb.search|#evaluating

The ratings will help you to determine if this is the right patch for your needs and whether or not it is necessary to apply those patches onto the system. You may not wish to take the risk of installing a patch with a low rating. You must understand these ratings so you can properly evaluate, select and download those patches that best suit your needs. HP has improved the process of selecting patches. It will automatically select all required dependencies. The patches are grouped and made available via a zip package/file for download onto your PC. Unzip the files and upload them to a temporary directory on the centralized local depot system via ftp.

Save the Bundle

Run the installation script provided by HP in the download and it will unpack the files and create a bundle called “BUNDLE”. A bundle is a set of patches grouped

together for a specific purpose. The bundle names have the following format, Name, Version and Description. The system administrator can modify the attributes of bundles making them applicable to the environment. Creating a bundle with consistent naming convention, description and version control number for ease of patch management. This will set up a standardized configuration procedure to be used by all system administrators using the standard install software tool SD-UX. For example, the name of the security bundle can be SamsSecurityBundle. Each time a new bundle is created with an increment in version number; i.e. 1.0, 1.1, 1.2 etc. The description should always include the date. For example:

SamsSecurityBundle 1.2 Mar-3-2003 Security Bundle

Bundles are complete unto themselves. The previous version is copied and a new bundle created with both new and previous patches so you will only have to install the latest version. Be sure to cleanup the newly created bundle by removing superseded patches. This decreases disk space required to store the patches and insures that you have a clean bundle.

Use the "make_bundles" command to create a new bundle with the properly formatted name as followed:

$ make_bundle –B –n {bundle name} –t "{Description}" –r {version} {depot}

HP also has a command "cleanup –d" to remove superceded patches in depots to free up disk space on the system.

Use the "swcopy" command to copy the newly created patch bundle to the proper centralized depot. Organize your bundles into depots. These depots can be arranged by OS level, patch only, application only etc. Since HP is supporting current OS versions of 11.0 and 11i. There can be separate depots for each OS version, 11.0 and 11.i applications and the 11.0 and 11i patches. Another reason for multiple depots is, it's less time consuming to perform system maintenance when installing, upgrading or applying patch bundles. Since each depot is complete, it can be applied as a whole instead of searching for specific patches or bundles.

Remove the Bundle

You can now delete the bundle created by HP's script with the following HP command.

$ swremove –d BUNDLE @ /tmp/patches/depot

The above command will remove the bundle called "BUNDLE" from the temporary depot.

Save the Text Files

Each patch comes with a text file. This text file contains important information about the patch and special instructions. This information must be also saved in a text files depot.

1. Create a listing of the patches in the new depot and save it with the text files.

$ swlist –l product –s /tmp/patches/depot > /tmp/patches/SamsSecurityBundle.1.2.text

2. Create a directory for the new bundle's text files. Text directories should have the same name as the bundle.

$ mkdir /{depot directory}.text/SamsSecurityBundle.1.2

3. Copy all of the ".text" files and the saved HP web page to this directory.

$ cp /tmp/patches/*.text /{depot directory}/SamsSecurityBundle.1.2
$ cp /tmp/patches/*htm /{depot directory}.text/SamsSecurityBundle.1.2

Cleanup Temporary Directory

Once the new bundle has been copied to the patch depot and the text files copied, you can delete the temporary working directory.

$ rm –r /tmp/patches

However, before installing any patches onto the HP servers, there are a few steps that must performed. First, a full system backup is required to ensure data recoverability. Second, create two make_recovery tapes, a vendor supplied tool for rebuilding your system. Finally, the patches must be installed on a test system prior to production systems. Testing the patch installation will enable you to prevent production system downtime due to the installation failing. After the patches have been successfully installed and sufficient time has past to prove the system stable, create a new make-recovery tape. This is done because kernel parameters changes may have been introduced. By having this new make-recovery tape, you will not have to re-apply the patches in the event the system needs to be rebuilt.

Conclusion

We chose HP-UX Security Patch Check from our vendor because we can easily obtain/download and install the software on our systems. There is no need for configuration and there is no cost in using this product. We found that Security Patch Check tool from HP is sufficient to use as our Security Patch Management tool for our HP servers. As long as we keep security patches and keep products up-to-date on our HP servers, the security vulnerability is minimal.

Even though HP provides this tool, it is only sufficient to identify the major security vulnerabilities. However, HP is changing their methodology for creating patches for applications. Instead if patching they are releasing new versions of their applications.

By upgrading and not patching applications, HP has added a new task to the system administrator's ever growing list of duties. Determining if the new release of an application is simply for features or includes security patches. This will greatly affect when applications are upgraded. In addition, applying new security patches might introduce new issues with the upgraded applications.

We realize that the patching process will always need to be analyzed by the system administrator. Each patch or application must be reviewed to determine if installing it is appropriate for the system. The Security Patch Check tool should include a listing of products that needs to be updated, i.e. Sendmail, SSH, Bind and others. These products are never patched but just replaced with a newer product. It would be helpful for the systems administrators to have an automated tool that would cover the vast majority of patch or product downloads and upgrades. Currently, the tool checks the system by comparing a catalog of patches to the installed patches on the server. HP could and should enhance the tool to add product updates to its capability by including the existing product catalog. This would greatly reduce the time spent on ensuring that the security and product patch levels are consistent and concurrent on the system and improve Security Patch Check's value to the system administrator.

Currently, this process meets our needs, assessments and willingness to assume risk. It's not a guarantee that new applications or new patches will not introduce other issues. It still requires that applications and other products be reviewed manually for security vulnerabilities.

This is by no means a static solution or process. Due to the business growing and constantly changing and along with the new technology, such as, hardware, networks, wireless, etc. being added to the environment this process will need to be adjusted. This process works today but might not be working 6 months from now. We need to continue to evaluate the process to be sure that it's still viable and meets the need of our business currently and in the future. Therefore, security vulnerabilities will always exist.

According to Steve Ulfelder in Network World, 10/21/02; Terry Grogan, manager of information systems security at Lancaster General Hospital in Pennsylvania, “agrees but accepts the inevitable”. "There's no perfect solution until we don't need to put them on," she says. "But for now, I still need to manually patch my systems, and I need to know what's out there." [5]

References

1. *Ulfelder, Steve: “Practical Patch Management”, Network World, 10/21/2002. URL: (www.nwfusion.com/supp/security2/patch.html)*

2. Ellen Messmer: “Patch management burdens customers”, Network World, 07/28/03, (http://www.nwfusion.com/news/2003/0728specialfocus.html)

3. **http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA**

4. **http://docs.hp.com/HP-UX/onlinedocs/5967-3578/5967-3578.pdf**

5. ***By Steve Ulfelder***
   Network World, 10/21/02
   (www.nwfusion.com/supp/security2/patch.html)

Appendix A: Sample run taken from HP's website.

http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA

This sample was generated by running **security_patch_check –r**

Implementing HP-UX Security Patch Check

Installation

2. Download Security Patch Check.
3. Verify Perl 5.005 or newer is installed. Perl must be installed before security_patch_check can be run. A pre-compiled version containing the necessary modules is available from Software Depot.
4. Install using HP-UX swinstall .

Configuration

- No manual configuration is needed.

Using the tool

Step 1: To determine which patches are missing from a system, Security Patch Check compares a catalog of security-related patches to the patches on your system. The tool must have local access to a catalog to work correctly, so the first thing you must do is get a copy of the catalog from the IT Resource Center (ITRC).

1. Run **security_patch_check -r**
   The tool will retrieve the latest catalog, analyze your system, and generate a listing of recommended patches.

Sample output

This sample was generated by running **security_patch_check -r**. Used this way the tool automatically downloads the Security Patch Check catalog, reporting on its progress as it

proceeds. It also warns about recalled patches and other security issues and generates a list of "recommended patches."

myPrompt> **/opt/sec_mgmt/spc/bin/security_patch_check -r**

NOTE: Downloading from ftp://ftp.itrc.hp.com.

NOTE: Downloading /export/patches/security_catalog.sync.

NOTE: /export/patches/security_catalog.sync downloaded to ./security_catalog.sync successfully.

NOTE: Downloading /export/patches/security_catalog.gz.

NOTE: /export/patches/security_catalog.gz downloaded to ./security_catalog.gz successfully.

NOTE: Recalled patch PHCO_16795 is present, but superseded by PHCO_20443 on the target system. If patch PHCO_20443 is ever removed, patch

WARNING: Recalled patch PHCO_14044 is active on the target system. Its record, including the Warn field, is available from ./security_catalog, through the

WARNING: Recalled patch PHCO_16795 is active on the target system. Its record, including the Warn field, is available from ./security_catalog, through the

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check, run as myuser
List of recommended patches for most secure system:

#	Recommended	Bull	Spec?	Reboot?	PDep?	Description

*** END OF REPORT ***
NOTE: Security bulletins can be found ordered by number at

NOTE: Security bulletins can be found ordered by number at
http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin

myPrompt>

Step 1: Identify, analyze and select recommended patches from www.itrc.hp.com.

Step 2: After downloading the selected patches, create a new patch bundle with version control for ease of management.

Apply new patches to a test system first. Before applying new patches to production or critical systems, make sure you have a full system backup and a make-recovery tape of root.

Step 3: Since security patches can be released at any time, the catalog used by Security Patch Check is updated nightly. You should create a policy and procedure for updating the catalog on a regular basis. The easiest way is to set up a cron job that runs nightly.

http://www.software.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=B6834AA

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor