



Security Updates

2 years of experience
with applying them
to DESY Linux 4

Stephan Wiesand

DESY Zeuthen - DV -

August 26, 2003

Note: Updates vs. Upgrades



- **Upgrades**
 - sometimes have to be applied
 - kernel with additional/updated drivers
 - XFree86 with additional/updated drivers
 - **should be avoided** within a major DESY Linux release
 - are rare within a SuSE/RedHat/debian release
- **Updates** as provided by the distributions
 - **fix severe bugs** with or w/o bugs on security
 - very little else
 - are **fixed** versions of the **initially** released packages
 - **not** the latest version from the software project

Note: Vulnerability Handling



- most serious threats handled by **CERT**
 - there are others caring for security as well
- **CERT policy:**
 - notify vendors of reported & confirmed vulnerabilities
 - SUN, HP, SGI, IBM, SuSE, RedHat, debian, MS,...
 - **most serious issues affect many vendors at once**
 - negotiate a time frame for releasing the information
 - give vendors **time to develop and test a compatible fix**
 - release advisory and vendor fixes at same time
- most problems are found by the good guys today

Vulnerability Handling



- hence, usually **once the updates are released**
 - there is a **confirmed problem**
 - there is at least a **confirmed possibility of exploits**
 - the **fix has been tested** by the distributors
- alternative ways of handling:
 - distributors do their own security audits
 - if they find something serious, they often contact CERT
 - but sometimes they go on their own
 - someone posts a hole he found (frequent)
 - some bozo posts a trivial root exploit (very rarely)



Handling in Zeuthen

- **monitor** relevant mailing lists (by 2 persons)
- when threats come up, **assess**
 - **relevance** and **risk** of the problem
 - **DOS** vs. **local/remote root/user exploit** (all can be serious)
 - **attacks possible from DESY? CERN? anywhere?**
 - **risk for stable stable operation** introduced by fix
- **policy: if in doubt, apply update** (frequent case)
- apply updates (or workarounds)
 - immediately on test hosts
 - usually later on general and critical system

Tools for RPM Handling



- **dzpm**
 - MySQL backend, command line frontend
 - knows about all packages ever relevant to DL4, DL5
 - works for available RPMs like rpm for installed RPMs
 - additionally, knows about **latest and best versions**
 - in general, **not necessarily the same**
 - from configuration files, hierachic, possibly host specific
 - **examples:**
 - `dzpm -q glibc` → ALL versions/releases
 - `dzpm -q --best glibc` → BEST version of glibc
 - `dzpm -q --latest glibc` → LATEST version/release



Tools for RPM Handling

- **dzpu**
 - deals with packages in configuration file
 - can **install** and **erase** packages
 - **upgrades** (or **downgrades**) to BEST version
 - only if installed
 - only if **age of package file** in work days is sufficient
 - 3 classes of hosts
 - minimum age configurable per package and class
 - only if configured **tags for a package** are met by c.l. args
 - **logs** all actions
 - **provides feedback** to caller (init script, cfengine)

Examples from Configuration



#name	arch	vers.	release	mode	age	tags
glibc	i386	2.2.2	68	U	1 2 5	boot
glibc-devel	i386	2.2.2	68	U	1 2 5	
glibc-profile	i386	2.2.2	68	U	1 2 5	
glibc-info	i386	2.2.2	68	U	1 2 5	
glibc-html	i386	*	*	e		
gpg	i386	1.0.6	193	U	0 0 0	
graphviz	i386	1.7.6	14	iU	0 0 0	userapp

- *glibc is only updated during reboot* (and then we'll reboot again)
 - if age is $\geq 1/2/5$ work days
- *glibc-html is deleted* if installed
- *graphviz is not installed on servers*

What Happened during 2 Years



- current default configuration has > 150 rows
 - more than 100 are fixes (some more than once)
- we apply all relevant updates released by SuSE
- we have never downgraded after an update
- all DL4 hosts at Zeuthen run identical releases
- we encountered one problem due to an update:
 - after a glibc update, NFS servers on slow hardware came up announcing to be capable of V2 only
 - slowed things down, but didn't break anything
 - cured by a few additional lines in /etc/init.d/nfsserver

Summary: The Future in Zeuthen



- we see **no reason to change our policy**
 - availability of **service for users is best with updates**
 - very **little additional downtime** (occasional reboots for glibc updates often coupled with kernel upgrade)
 - how many mysterious crashes are failed exploits?
 - **occasional hiccup better than 1-week shutdown**
 - after infestation of institute by hackers
 - **SuSE's updates are good**
 - security patches are the major point in using a distribution at all
 - **minor improvements foreseen**
 - run updates also during shutdown, not only boot
 - pre-/post-actions for dzpu