Estate Valuations and Pricing Systems, Inc.
Patch Management Process

Summary

EVP Systems maintains two primary technical infrastructures—desktop workstations and data-center servers—and the operating systems and applications used by both require regular upgrades and patches. This document describes the process used to install these changes.

Monitoring

All EVP Systems computers are regularly monitored not only for security breaches but for the availability of patches and upgrades that implement both improved security and new functionality.

On the company's data center servers, running the Ubuntu distribution of Linux, the primary method of patch awareness is via the OS's `apt` subsystem, which checks central servers provided by the vendor for upgrades. On the Windows 10 workstations, Windows Update provides the same functionality.

Additionally, news sources and on-line resources are regularly monitored for important or significant security issues for both primary operating systems and major applications.

Once a month, EVP Systems runs security assessments—as defined by the "Intrusion Detection and Audit Process" document—and any anomalous behavior detected by the audit may also prompt a patch.

Assessment and Prioritization

When a patch is either recommended by the vendor as part of their main upgrade path, or determined to be relevant to the EVP Systems technical infrastructure by company technical staff, it is applied as soon as possible. The target application time is within 24 hours of discovery.

Microsoft Office is upgraded via Windows Update, the exact same was as Windows itself. Other applications—including EVP Systems own EVP Office—are upgraded and patched on an as-needed basis, or when the workstation is rebuilt, annually, as per the "Security Information Policy" documentation.

Testing

Patches provided by the operating system vendor as part of their main upgrade path are assumed good, and applied without additional EVP Systems testing. Non-standard patches that EVP Systems have determined are important are first applied to test systems—both for Ubuntu and Windows—and then rolled into production if no negative side-effects manifest.

Automated Implementation

Windows patches and upgrades are applied automatically by the operating system weekly, during a window of no user activity. If a reboot is required, the Windows workstations restart themselves outside of business hours.

TheUbuntu servers patch themselves nightly, during a window between 1:00 and 2:00am, Pacific Time. If a reboot is required, the servers reboot themselves during the maintenance window. However, since each server has a fully functional twin and a load-balancer that distributes requests between them, staggered restarts prevent any downtime.

Manual Implementation

If the operating system's vendors do not provide an officially approved patch for a particular issue, or do not elevate it to the priority that is automatically installed, EVP Systems technical staff will manually install the upgrade, during non-business hours, ideally on a weekend. Server patches are applied across a functional pair of servers independently, so they require no downtime.

Documentation

All patches automatically applied to the Linux servers are recorded in `/var/log/apt/history.log*`, a set of files that lists the date and name of each upgraded package.

Automatically applied patches to the Windows 10 workstations can be listed by going to `Settings` → `Update & security` → `Update history`.

Manually applied patches are recorded in the "Internet Vulnerability Responses" document.

Last Updated: September 3, 2019