Estate Valuations & Pricing Systems, Inc.
Internet Vulnerability Responses

Summary

This document describes the responses Estate Valuations & Pricing Systems, Inc. has made to several high-profile Internet security vulnerabilities. For each issue, any vendor fix was applied the day the patch became available. No breaches have occurred, and no company or client data has been compromised. (See “Intrusion Detection and Audit Process.”)

Heartbleed / CVE-2014-0160

When Heartbleed (officially designated CVE-2014-0160) was announced in April 2014, EVP Systems ran Ubuntu 10.04 LTS servers. Though the company did not use the affected SSL/TLS technology, the vendor’s patch was applied within eight hours, per good security hygiene.

Shellshock / Bashdoor / CVE-2014-6271

Shellshock (also known as Bashdoor, CVE-2014-6271 and other related CVEs) was announced in September 2014. EVP Systems ran Ubuntu 10.04 LTS servers at the time, and applied vendor patches both shortly after the original announcement and in the subsequent days as other, related vulnerabilities were discovered and fixed. No unauthorized access or commands were run as a result of Shellshock.

POODLE / CVE-2014-3566

Like Heartbleed, POODLE (aka CVE-2014-3566, announced in September 2014) attacks SSL/TLS technology not used by the EVP infrastructure, but vendor patches were applied the day they became available. Related, all in-company browsers were updated to remove SSLv3 fallback behavior.

MS14-066 / Winshock / CVE-2014-6321

When MS14-066 was announced in November 2014, EVP Systems did not use Microsoft servers, so no remediation in the data center was required. Desktop installations of Windows were patched as part of the normal, automated upgrade cycle.

GHOST / CVE-2015-0235

GHOST is a buffer-overflow vulnerability in the domain name resolution functions in glibc, and a properly constructed attack could cause any program that uses those functions on externally provided data to crash. (The EVP Apache Web server, for instance, fits this description, as a requesting-hostnames are reverse-resolved for logging.) A vendor-provided patch was applied within 24 hours of the vulnerability being announced in January 2015, and no attacks using GHOST were used against EVP servers.

Juniper Router Compromise / CVE-2015-7755, CVE-2015-7756

Backdoors surreptitiously installed in the firmware of routers produced by Juniper Networks were announced in December 2015, and have potentially been available since 2012. EVP Systems does not use Juniper hardware and was not affected by these compromises.

Struts 2 / CVE-2017-5638

On March 6, 2016, a vulnerability in the Apache Foundation's Struts 2 framework was announced, as CVE-2017-5638. EVP Systems does not use Struts and was unaffected by the issue.

Tomcat Remote Execution / CVE-2017-12615

On September 20, 2017, a remote execution exploit was announced for the Apache Foundation's Tomcat server, as CVE-2017-12615. The vulnerability affected Tomcat 7.0.0 to 7.0.79, running on Windows servers. EVP Systems does not use Tomcat 7 or Windows servers, and so was unaffected by the issue.

Dnsmasq Overflow / CVE-2017-14491 (and Related)

On October 2, 2017, seven different flaws in the Dnsmasq package were announced, as CVE-2017-14491 through CVE-2017-14496. EVP Systems does not use Dnsmasq, and was unaffected by the issue.

Spectre and Meltdown / CVE-2017-5715, CVE-2017-5753; CVE-2017-5754

On January 3, 2018, two vulnerabilities in all modern CPUs were made public: Spectre (CVE-2017-5715 and CVE-2017-5753) and Meltdown (CVE-2017-5754). EVP Systems completed the installation of vendor-provided mitigations for these flaws -- for both their cloud-based data center servers and desktop machines -- on January 13, 2018.

EVP Systems' servers all run the Ubuntu 16.04 operating system. A vendor-provided kernel that prevents the CPU from being exploited by the flaws was made available on January 9, 2018 and applied during the next maintenance window, on January 13, 2018.

All EVP Systems' Windows desktop machines automatically apply patches nightly via Windows Update, and received the fix (KB4056892) the night of January 4, 2018. All Macs were upgraded to macOS 10.13.2 with the supplemental security patch release on January 9, 2018.

EVP Systems does not issue cell phones or other devices to its employees, but has provided technical assistance so their personal systems can be safely upgraded. In addition to the Windows and macOS upgrades for employee's own computers, the company has recommended that iPhones be upgraded to iOS 11.2.2 (as of January 8, 2018) and that Android owners contact their vendor to get a patch designed for their specific device.

EVP Systems other CPU-based machines -- its printers, scanners, routers, and alarm and phone systems -- do not have vendor-provided patches available yet, though since these devices are all run purpose-specific operating systems and are not designed to be either virtualized or to execute arbitrary code, the risk of exploitation is nearly non-existent. However, part of the company's monthly security review will now include checking vendor sites, and updated operating systems or firmware will be applied if and when they are released.

libSSH / CVE-2018-10933

On October 17, 2018, a vulnerability in the libSSH library was announced, as CVE-2018-10933, that allowed third-parties to log into servers running the code without any authorization. EVP Systems does not use libSSH in either its own code or in the other software running on its servers, and was not affected.

Citrix Netscaler / CVE-2019-19781

In December 2019, a severe vulnerability in the Citrix environment was announced, as CVE-2019-19781, allowing directory traversal on Citrix servers. EVP Systems does not use Citix, and was not affected.

Windows CryptAPI / CVE-2020-0601

On January 14, 2020, Microsoft announced a severe vulnerability in the Windows CryptAPI functionality, as CVE-2020-0601, that allows unverified remote code execution. EVP Systems uses a vulnerable Microsoft operating system, Windows 10, and applied the patch as part of our nightly security updates as soon as it was available, on January 15, 2020.

SUNBURST / CERT Emergency Directive 21-01

In December 13, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) Computer Emergency Readiness Team (CERT) issued Emergency Directive 21-01, which announced the existence of a supply-chain back-door into SolarWinds popular network administration tool. EVP Systems uses a SolarWinds product — Papertrail — to monitor output logs, but it was not affected by the exploit. Papertrail is a remote storage and filtering mechanism, and does not run on EVP Systems servers. Further, the software that sends data to Papertrail is open source (https://github.com/papertrail/remote_syslog2), and was last updated on June 14, 2019, before SolarWinds supply chain was breached. Thus, no mitigation was required.

Baron Samedit / CVE-2021-3156

In January 2021, a bug in the “sudoedit” root-permission access program on many UNIX variants—including the Ubuntu Linux that EVP Systems uses—was announced. By running a certain command as a low-level user, administrative access would be granted. However, EVP Systems installs security patches from the vendor every night, and so the fix was automatically applied on as soon as it was available, on January 26, 2021.

HAFNIUM / Exchange Marauder / CVE-2021-26855

In March 2021, Microsoft’s Exchange server software was widely compromised by a server-side request forgery, allowing other bugs in the system to be exploited. EVP Systems does not use Exchange, and was therefore unaffected.

log4shell / CVE-2021-26855, CVE-2021-45046, CVE-2021-45105

On December 10, 2021, log4j—the popular logging library for Java—was discovered to have a severe remote code execution (RCE) bug in versions 2.0 and greater. Sending a specific string of characters to a program using log4j would allow any commands to be run on the targeted system. The initial patch to the library was unsuccessful, so another was released. That change exposed an infinite-recursion denial-of-service attack bug. EVP Systems does not use log4j in any of its software save one internal system, and it has repeatedly been upgraded to the latest log4j version.

Last update: December 20, 2021