ActivePerl®

OPEN SOURCE SECURITY:

ENTERPRISE RISKS OF UNSUPPORTED PERL

Millions of developers and enterprises around the world trust Perl for mission critical business tasks in system administration, databases, and security. But what is the real cost of open source, and can it be measured in dollars alone?

Open source Perl is not commercially backed or supported. Security, stability, and reliability is paramount, and enterprises cannot (and should not) rely on it to run critical processes that keep their businesses running. Anything less could result in security lapses, business failures, costly downtime, and incalculable loss to business reputations and relationships, not to mention development cycles and money.

Since 2005, ActiveState has applied 28 security patches to ActivePerl and has made many routine updates to OpenSSL and other security-critical libraries as provided by the community. Refer to the table below and see how ActiveState routinely protects its customers from security vulnerabilities, both minor to potentially catastrophic.

ISSUE	DESCRIPTION	IMPACT TO ENTERPRISES
CVE-2016-0800	Cross-protocol attack on TLS using SSLv2 (DROWN) (HIGH)	The DROWN attack allows attackers to break encryption on HTTPS and get access to all communications.
CVE-2016-0705	Double-free in DSA code (low)	Denial of service, with the potential for further effects depending on the complexity of the attack
CVE-2016-0798	Memory leak in SRP database lookups (low)	Denial of service
CVE-2016-0797	BN_hex2bn/BN_dec2bn NULL pointer deref/heap (low)	Denial of service, with the potential for further effects depending on the complexity of the attack
CVE-2016-0799	Fix memory issues in BIO_*printf functions (low)	Denial of service, with the potential for further effects depending on the complexity of the attack
CVE-2016-0702	Side channel attack on modular exponentiation (low)	Local attack that could reveal RSA keys to another user on the same machine, allowing them to decrypt other user's communications
CVE-2016-2381	Context-dependent attack to bypass taint protection (medium)	Allows user data to bypass "taint" checking, which could allow SQL injection attacks (table deletion etc) on application databases
CVE-2015-3193	BN_mod_exp may produce incorrect results on (medium)	Weakens keys in ways that may allow their discovery, allowing remote attackers to decrypt communications from affected systems
CVE-2015-3194	Certificate verify crash with missing PSS (HIGH)	Denial of service by very simple attack to crash server
CVE-2015-3195	X509_ATTRIBUTE memory leak (medium)	Remote attackers can gain access to process memory (similar to Heartbleed)
CVE-2015-3196	Race condition handling PSK identify hint (medium)	Denial of service
CVE-2015-1794	Anon DH ServerKeyExchange with 0 p parameter (medium)	Denial of service
CVE-2015-8608	out-of-bounds read and over-read vulnerabilities	Remote attacker could execute arbitrary code on target system, allowing access to private information on the system
CVE-2014-0160	Heartbleed (medium)	Remote attacker could undetectably read any number of random blocks of memory, potentially revealing passwords or other confidential information
CVE-2014-0076	Cache Side-channel Attack (low)	Local attacker could discover secret key ("nonce") used to encrypt communications, allowing decryption

ActivePerl® Business Edition

For enterprises concerned with security, efficiency, and performance, ActiveState's precompiled open source language distributions are the only answer. They provide the reliability and quality that enterprises need to ensure proper security protocols are followed and implemented.

ActivePerl Enterprise Edition customers receive quarterly updates for all their builds unless there is an open source security issue that is urgent and will have significant impact. Those fixes will be provided on an ad hoc basis. This provides enterprises with the peace of mind that their products will always be secure and up-to-date. For Business Edition customers, issues will be fixed in our next regularly scheduled releases, unless there is a severe security issue which could result in a special patch release.

This is why large enterprises like CA, Siemens, and Boeing trust ActiveState's ActivePerl for end-to-end Perl development, management and distribution solutions. ActivePerl is a commercial-grade, fully tested and supported Perl distribution used by companies around the world for easy Perl installation and quality-assured code. ActiveState takes on the responsibility of maintaining and supporting ActivePerl and ensures that all security fixes are applied quickly, safely, and with quality–usually faster than open source Perl. Please contact us at solutions@activestate.com to learn more.

ActiveState Software Inc.
solutions@activestate.com

Phone: **+1.778.786.1100**
Fax: **+1.778.786.1133**

Toll-free in North America:
1.866.631.4581

ActiveState®

ABOUT ACTIVESTATE

ActiveState, the open source languages company, believes that enterprises gain a competitive advantage when they are able to quickly create, deploy and efficiently manage software solutions that immediately create business value, but they face many challenges that prevent them from doing so. The company is uniquely positioned to help address these challenges through our experience with enterprises, developers and open source technology. ActiveState is proven for the enterprise: more than 2 million developers and 97 percent of Fortune 1000 companies use ActiveState's end-to-end solutions to develop, distribute, and manage their software applications written in Perl, Python, Ruby, Go, Node.js, Lua, Tcl and other dynamic languages. Global customers like Cisco, CA, HP, Bank of America, Siemens and Lockheed Martin trust ActiveState to save time, save money, minimize risk, ensure compliance, and reduce time to market. To learn more visit, ActiveState.com.