

OpenSSL Vulnerability Shows Open-Source Process Weaknesses

John Pescatore

A major security flaw in some Linux distributions could expose encrypted data. Open-source developers and their vendor counterparts must improve their communications processes to address security issues like this one.

NEWS ANALYSIS

Event

On 16 May 2008, the SANS Institute issued a "yellow alert" concerning a recently discovered Secure Sockets Layer (SSL) security vulnerability in some Debian distributions of the Linux operating system. The vulnerability, which affects encryption key pairs used by the Debian OpenSSL package, could enable unauthorized parties to access encrypted transaction data, passwords, financial information and other sensitive data. A Debian advisory offers recommendations for patching the software and regenerating the encryption keys (see www.debian.org/security/2008/dsa-1571).

Analysis

This vulnerability — which was apparently introduced by Debian's developers, not open-source OpenSSL developers — highlights one of the risks of using software products that incorporate open-source modules. In May 2006, the Debian developers chose to make changes to the OpenSSL package used in Debian to fix what appeared to be a memory leak, rather than wait for the OpenSSL developer community to investigate and address the issue. The Debian "fix" resulted in a serious weakness in the OpenSSL random-number generator that made it easy for attackers to discover encryption keys. In general, encryption code should not be modified without a very thorough process designed to determine the impact of the modifications, both on the proper functioning of the code and on Federal Information Processing Standards (FIPS) compliance status.

According to postings to the OpenSSL developers' mailing list, the Debian developers made a good-faith attempt to communicate with the OpenSSL development community, but informal communication processes were clearly inadequate in this instance. (Gartner repeatedly attempted to contact Debian concerning this First Take, but was unable to do so. We believe this experience confirms our view that open-source process communications require significant improvements.) In many other cases, product vendors have made changes to open-source packages without even attempting to contact the "upstream" developers. This approach significantly increases both the risk that new vulnerabilities will be introduced into open-source code and the likelihood that upstream fixes for other vulnerabilities will cause later problems with the vendor-modified modules. Both commercial and open-source vendors frequently incorporate third-party open-source modules in their code, so enterprises need to be aware of the potential issues that can result.

RECOMMENDATIONS

- **Open-source communities:** Establish a standardized communication process for vendor communications with open-source development teams, comparable to many commercial vendors' standardized use of [www.\[companyname\].com/security](http://www.[companyname].com/security) to host mailboxes for reporting vulnerabilities.
- **Enterprises using the affected Debian versions:** Follow the recommendations of the Debian advisory to patch software and regenerate all cryptographic keys generated by Debian OpenSSL versions beginning with 0.9.8c-1.
- **All enterprises:** Ensure that your vulnerability management processes include an inventory of applications (both proprietary and open source) to identify any open-source software dependencies and ensure that all modules are at current patch levels.

RECOMMENDED READING

- "Findings for Gartner Open Source Summit: Integrate Vulnerability Assessment With Open-Source License Management Tools" — Integrating vulnerability assessment capabilities into open-source license management tools is a low-cost way to increase open-source security. **By John Pescatore**
- "Hype Cycle for Open-Source Software, 2007" — Open-source software continues to mature across a broad spectrum of market segments, but with highly variable maturity rates and saturation levels. **By Mark Driver and others**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509