Bleeding Heart Computer Security

Every day the Internet is a battlefield where cyber security black hats and white hats fight for control of your computer. Some days the good guys win. Some days the bad guys win. And some days it isn't clear that anybody wins. But one thing is for sure, computer security is something that can only be ignored with great risk, and it is likely that it will only become more critical to you and your business as time marches on.

BASIS is committed to monitoring and responding to computer security issues as they are detected. Occasionally a major security issue is announced that requires immediate action – such was the case with the Heartbleed Vulnerability.

Heartbleed Vulnerability

The Heartbleed Vulnerability was a major security issue that was announced in April 2014 as "CVE-2014-0160," where CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by the MITRE Corporation.

Heartbleed was essentially a security hole in versions 1.0.1 through 1.0.1f of an Open Source encryption library called OpenSSL. If an attacker could open a connection to a service using an affected version of OpenSSL, the security hole allowed the attacker to extract random data from a memory buffer that might contain sensitive data such as passwords and encryption keys.

"*The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.*" heartbleed.com

When the news came out about Heartbleed, our immediate concern at BASIS was to determine what impact Heartbleed might have on customers using our product line. Heartbleed required an immediate investigation and an immediate response.

Our investigation showed that BBj® was not affected. The only BBj component that used OpenSSL was an ODBC client for Windows, which has both a 32-bit and a 64-bit version. At that time the 32-bit version was using OpenSSL 0.9.x, which was

By Dan Christman
Software Engineer

By Jerry Karasz
Software Architect

unaffected by Heartbleed, but the 64-bit version was using OpenSSL 1.0.1c and was potentially at risk. Further investigation showed, however, that the 64-bit ODBC client was not vulnerable to the Heartbleed issue because Heartbleed only affected software that would accept incoming socket connections.

The investigation also showed that PRO/5® and Visual PRO/5® used OpenSSL for SSL sockets, but that the OpenSSL version being used was 0.9.x, which was unaffected by Heartbleed. Having determined from our investigation that no action was needed on BASIS' part, and that all was right with the world, we announced our results and went back to our development tasks secure in the knowledge that Heartbleed was not our problem.

Reverse Heartbleed Vulnerability

And then came the Reverse Heartbleed announcement. Reverse Heartbleed was a security hole similar to Heartbleed that allowed a malicious server that accepted a connection from a vulnerable client to extract random data from the client's memory buffer (that is why it is referred to as the "reverse"). Reverse Heartbleed could only be exploited by tricking a vulnerable client into connecting to a malicious server, a situation that was not as common as the Heartbleed vulnerability. Back to work to investigate the BASIS product line yet again.

The investigation showed that the 64-bit BBj ODBC client for Windows was the only product that offered any possible vulnerability to Reverse Heartbleed. Since it was just barely possible that a malicious server could steal sensitive information by tricking a client into using a BBj 64-bit ODBC client to connect to it, we upgraded the 64-bit ODBC DLL to the latest OpenSSL version. We released an updated 64-bit ODBC DLL for those who might need to patch an older version of the BBj 64-bit ODBC client for Windows without upgrading to the latest version of BBj, and created a knowledge base article *Heartbleed Fix for 64-bit Windows BBj ODBC Driver* to help customers understand the issue.

Proactive Updates

Even though PRO/5, Visual PRO/5 and the 32-bit BBj ODBC client for Window were never affected by Heartbleed or Reverse Heartbleed, BASIS upgraded the OpenSSL library that those products use to the latest version that contained the official fix for those vulnerabilities.

Besides the potential language impact, Heartbleed brought an operating system compliance cost. BASIS' Transformer AMI (Amazon Machine Image) includes a version of OpenSSL, and Amazon Marketplace insisted on a full upgrade to OpenSSL version 1.0.1g. Shortly thereafter, they required a second compliance upgrade to OpenSSL version 1.0.1h.

In today's compliance-driven world, it is important to remain current with the most secure versions of the software upon which your business relies. BASIS' Transformer AMI has a compliant OS, and the newer versions of BASIS products ship with a current version of OpenSSL that contains the official fix for both vulnerabilities.

Summary

The BASIS product line was never affected by the Heartbleed vulnerability because its only affected component could not accept incoming socket connections. The 64-bit ODBC DLL that had a vulnerable version of OpenSSL was affected by Reverse Heartbleed in that it cannot accept incoming connections.

Computer security is a constant battle. Everyone can make a mistake, as the developers of the OpenSSL library did. The important thing is that we all remain vigilant and on the lookout for as many of these problems that we can and work to address them as quickly as possible.

Remember, if your applications use an OpenSSL library with version 1.0.1 through 1.0.1f (inclusive) for socket communications, you should review the information about Heartbleed and Reverse Heartbleed and investigate your programs for yourself. You may have created a security issue of your own. Meanwhile, we at BASIS will continue to watch for potential security issues in our product line and work to keep you informed and up to date. Keep your BASIS products updated to be secure! ■

For more details, refer to the knowledge base article *Heartbleed Fix for 64-bit Windows BBj ODBC Driver*