

## SSL360 Appliance OpenSSL Component Vulnerabilities

<b>Date discovered</b>	28 September 2006
<b>Bulletin issued</b>	AK-2006-08 1.1 (10 October 2006)
<b>Importance</b>	High Risk
<b>Impact</b>	Denial of service
<b>Level of competence required to launch an attack</b>	Expert
<b>Source of the attack</b>	Authorized networks
<b>How widely available?</b>	Widely available
<b>SSL360 SSL VPN Server releases</b>	All releases prior to 2.0/3

### Introduction

Multiple vulnerabilities have been uncovered in the OpenSSL component of the SSL360 system which could be used by an attacker to unnecessarily increase system resource usage.

### Description

Multiple implementation errors in the OpenSSL component could allow a denial of service attack based on the use of forged X.509 certificates for the establishment of SSL connections.

### Impact

An attack would lead to additional loading of system resources (CPU, memory), impacting system performance.

### Risk

This vulnerability is classed as **High Risk** for the following reasons:

- Denial of service ;
- Under certain conditions Internet-based attacks are possible.



## References

- OpenSSL Security Advisory ([http://www.openssl.org/news/secadv\\_20060928.txt](http://www.openssl.org/news/secadv_20060928.txt))
- CVE-2006-2937 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937>)
- CVE-2006-2940 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940>)

## Impacted Versions

- Major release 1.0: All versions (no longer supported)
- Major release 2.0: <= 2.0/2

## Solution

Release 2.0/3 corrects this problem. If your configuration is impacted we recommend updating the system as soon as possible

Note: Support for SSL360 version 1.0 was discontinued with the release of version 2.0/1. If you are using this an older release we recommend you upgrade to version 2.0/3 (or later) as soon as possible.

If you have any problems, contact the Arkoon support team via our web site at <http://client.arkoon.net>

Best regards

Arkoon Security Team  
[security@arkoon.net](mailto:security@arkoon.net)

