

## RSA signature verification vulnerability in OpenSSL

<b>Date discovered</b>	05 September 2006
<b>Bulletin issued</b>	AK-2006-04 1.1 (22 September 2006)
<b>Importance</b>	Medium Risk
<b>Impact</b>	By-passing of security policies
<b>Level of competence required to launch an attack</b>	Expert
<b>Source of the attack</b>	Internet
<b>How widely available?</b>	Easily available
<b>SSL360 SSL VPN Server releases</b>	All releases prior to 2.0/3

### Introduction

A vulnerability in the OpenSSL component responsible for verifying RSA signatures in SSL360 appliances has been detected. An exploit could allow an attacker to by-pass X.509 trust relationships.

Only configurations where the SSL360 appliance uses a certificate issued by a PKI for authentication are potentially impacted.

See the section "Identifying Vulnerable Configurations" below to find out if your appliances are impacted.

### Description

In deployments based on a Certificate Authority, the SSL360 appliance verifies user X.509 certificates using the CA certificate.

An implementation error potentially allows an attacker to use a forged certificate apparently signed by the CA, when an RSA key with exponent 3 is used. Password authentication is still obligatory in this case.

Note: This type of key is rarely used. The default certificates of SSL360 appliances, and the certificate authorities of Arkoon FAST360 UTM appliances, do not use this type of exponent.



## Impact

In configurations where user certificate authentication is activated and the CA certificate uses an RSA key with exponent 3, this vulnerability could allow an attacker to by-pass certificate verification and access the authentication window.

## Risk

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

- Allows security policies to be by-passed (certificate authentication);
- but does not allow authentication on the SSL360 appliance without the user password.

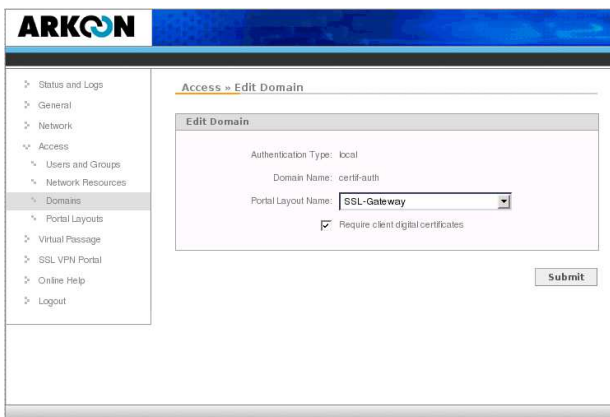
## Identifying Vulnerable Configurations

### Impacted versions:

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

### Impacted Configurations:

- Certificate-based user authentication activated, with a PKI using RSA keys with exponent 3.



Activating certificate-based user authentication

```
# openssl x509 -in /var/httpd/cacerts/cacerts.pem -noout -text
...
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
  Modulus (1024 bit):
    00:b6:1b:3d:8a:b7:24:18:21:4c:c5:07:26:b5:2d:
    a4:2d:26:ef:5f:dc:66:91:1d:53:dc:86:06:19:d3:
    50:4a:75:1d:9d:18:80:d8:0d:af:16:db:dd:2b:07:
    fe:a4:7b:c1:ef:45:7f:1b:6a:1b:7b:ae:24:4b:1f:
    43:bc:42:0b:08:ac:12:4c:c8:42:47:72:50:fc:ce:
    68:14:b9:9d:c4:4e:d1:1e:c5:74:9b:9d:15:b4:cb:
    b9:1c:e5:90:6e:f8:e0:97:76:00:f3:cf:34:75:22:
    df:71:04:96:79:cb:54:1b:ff:e9:89:d1:44:17:a3:
    b5:c9:56:6f:d7:1d:e6:27:df
  Exponent: 3 (0x3)
...
```

Certificate using an RSA key with exponent 3

## References

- OpenSSL Security Advisory ([http://www.openssl.org/news/secadv\\_20060905.txt](http://www.openssl.org/news/secadv_20060905.txt))
- CVE-2006-4339 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339>)



## 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)

