

# [Full-disclosure] Debian OpenSSL vulnerability – major CAs unaffected

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-05/msg00419.html>

---

- *From:* Alexander Klink <a.klink@xxxxxxxx>
  - *Date:* Thu, 15 May 2008 14:10:52 +0200
- 

Hi,

some good news in the whole Debian OpenSSL vulnerability mess:  
We have tested all the CAs with 1024 and 2048 bit keys with a public exponent of 65537 which are included in the Windows or Mozilla CA store against our list of known weak keys, but none of them were affected.

Not that we expected that they were, but we thought it might be better to check ;–)

A minor 13% has not been tested because they were using different key lengths or public exponents ...

Cheers,  
Alex

–

Dipl.–Math. Alexander Klink | IT–Security Engineer | a.klink@xxxxxxxx  
mobile: +49 (0)178 2121703 | Cynops GmbH | <http://www.cynops.de>

---

HRB 7833, Amtsgericht | USt–Id: DE 213094986 | Geschäftsführer:  
Bad Homburg v. d. Höhe | | Martin Bartosch

---

Full–Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>