



# CVE-2010-0928

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2010-0928
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-03-05 19:30:00 UTC
<b>Updated</b>	2023-11-07 02:05:00 UTC
<b>Description</b>	OpenSSL 0.9.8i on the Gaisler Research LEON3 SoC on the Xilinx Virtex-II Pro FPGA uses a Fixed Width Exponentiation (

## Risk And Classification

**Problem Types:** CWE-310

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Gaisler</a>	<a href="#">Leon3 Soc</a>	All	All	All	All
Hardware	<a href="#">Gaisler</a>	<a href="#">Leon3 Soc</a>	All	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8i	All	All	All
Hardware	<a href="#">Xilinx</a>	<a href="#">Virtex-ii Pro Fpga</a>	All	All	All	All
Hardware	<a href="#">Xilinx</a>	<a href="#">Virtex-ii Pro Fpga</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="http://www.eecs.umich.edu/~Evaleria/research/publications/DATE10RSA.pdf">www.eecs.umich.edu/~Evaleria/research/publications/DATE10RSA.pdf</a>	MISC	<a href="http://www.eecs.umich.edu">www.eecs.umich.edu</a>	Exploit
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
Researchers find way to zap RSA security scheme	MISC	<a href="http://www.networkworld.com">www.networkworld.com</a>	
62808	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>	
Attacking RSA exponentiation with fault injection « root labs rdist	MISC	<a href="http://rdist.root.org">rdist.root.org</a>	
'Severe' OpenSSL vuln busts public key crypto • The Register	MISC	<a href="http://www.theregister.co.uk">www.theregister.co.uk</a>	
<a href="http://www.eecs.umich.edu/~valeria/research/publications/DATE10RSA.pdf">www.eecs.umich.edu/~valeria/research/publications/DATE10RSA.pdf</a>		<a href="http://www.eecs.umich.edu">www.eecs.umich.edu</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical



### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-03-08	Mark Cox	CVE-2010-0928 describes a fault-based attack on OpenSSL where an attacker has precise control over the application's execution flow.



There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)