CVE-2010-0928

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2010-0928
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-05 19:30:00 UTC
Updated	2023-11-07 02:05:00 UTC
Description	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	Gaisler	Leon3 Soc	All	All	All	All
Hardware	Gaisler	Leon3 Soc	All	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Hardware	Xilinx	Virtex-ii Pro Fpga	All	All	All	All
Hardware	Xilinx	Virtex-ii Pro Fpga	All	All	All	All

References

Reference	Source	Link	Tags
www.eecs.umich.edu/%7Evaleria/research/publications/DATE10RSA.pdf	MISC	www.eecs.umich.edu	Exploit
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Researchers find way to zap RSA security scheme	MISC	www.networkworld.com	
62808	OSVDB	www.osvdb.org	
Attacking RSA exponentiation with fault injection « root labs rdist	MISC	rdist.root.org	
'Severe' OpenSSL vuln busts public key crypto • The Register	MISC	www.theregister.co.uk	
www.eecs.umich.edu/~valeria/research/publications/DATE10RSA.pdf		www.eecs.umich.edu	
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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 cont

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