CVE-2016-2849

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-2849
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-13 14:59:00 UTC
Updated	2017-07-01 01:29:00 UTC
Description	Botan before 1.10.13 and 1.11.x before 1.11.29 do not use a constant-time algorithm to perform a modular inverse on the s

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Botan Project	Botan	1.10.12	All	All	All
Application	Botan Project	Botan	1.11.0	All	All	All
Application	Botan Project	Botan	1.11.1	All	All	All
Application	Botan Project	Botan	1.11.10	All	All	All
Application	Botan Project	Botan	1.11.11	All	All	All
Application	Botan Project	Botan	1.11.12	All	All	All
Application	Botan Project	Botan	1.11.13	All	All	All
Application	Botan Project	Botan	1.11.14	All	All	All
Application	Botan Project	Botan	1.11.15	All	All	All
Application	Botan Project	Botan	1.11.16	All	All	All
Application	Botan Project	Botan	1.11.17	All	All	All
Application	Botan Project	Botan	1.11.18	All	All	All
Application	Botan Project	Botan	1.11.19	All	All	All
Application	Botan Project	Botan	1.11.2	All	All	All
Application	Botan Project	Botan	1.11.20	All	All	All
Application	Botan Project	Botan	1.11.21	All	All	All
Application	Botan Project	Botan	1.11.22	All	All	All

Application	Botan Project	Botan	1.11.23	All	All	All
Application	Botan Project	Botan	1.11.24	All	All	All
Application	Botan Project	Botan	1.11.25	All	All	All
Application	Botan Project	Botan	1.11.26	All	All	All
Application	Botan Project	Botan	1.11.27	All	All	All
Application	Botan Project	Botan	1.11.28	All	All	All
Application	Botan Project	Botan	1.11.3	All	All	All
Application	Botan Project	Botan	1.11.4	All	All	All
Application	Botan Project	Botan	1.11.5	All	All	All
Application	Botan Project	Botan	1.11.6	All	All	All
Application	Botan Project	Botan	1.11.7	All	All	All
Application	Botan Project	Botan	1.11.8	All	All	All
Application	Botan Project	Botan	1.11.9	All	All	All
Application	Botan Project	Botan	1.10.12	All	All	All
Application	Botan Project	Botan	1.11.0	All	All	All
Application	Botan Project	Botan	1.11.1	All	All	All
Application	Botan Project	Botan	1.11.10	All	All	All
Application	Botan Project	Botan	1.11.11	All	All	All
Application	Botan Project	Botan	1.11.12	All	All	All
Application	Botan Project	Botan	1.11.13	All	All	All
Application	Botan Project	Botan	1.11.14	All	All	All
Application	Botan Project	Botan	1.11.15	All	All	All
Application	Botan Project	Botan	1.11.16	All	All	All
Application	Botan Project	Botan	1.11.17	All	All	All
Application	Botan Project	Botan	1.11.18	All	All	All
Application	Botan Project	Botan	1.11.19	All	All	All
Application	Botan Project	Botan	1.11.2	All	All	All
Application	Botan Project	Botan	1.11.20	All	All	All
Application	Botan Project	Botan	1.11.21	All	All	All
Application	Botan Project	Botan	1.11.22	All	All	All
Application	Botan Project	Botan	1.11.23	All	All	All
Application	Botan Project	Botan	1.11.24	All	All	All
Application	Botan Project	Botan	1.11.25	All	All	All
Application	Botan Project	Botan	1.11.26	All	All	All
Application	Botan Project	Botan	1.11.27	All	All	All

Application	Botan Project	Botan	1.11.28	All	All	All
Application	Botan Project	Botan	1.11.3	All	All	All
Application	Botan Project	Botan	1.11.4	All	All	All
Application	Botan Project	Botan	1.11.5	All	All	All
Application	Botan Project	Botan	1.11.6	All	All	All
Application	Botan Project	Botan	1.11.7	All	All	All
Application	Botan Project	Botan	1.11.8	All	All	All
Application	Botan Project	Botan	1.11.9	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 24 Update: botan-1.10.13-1.fc24	FEDORA	lists.fedoraproject.org	
Debian -- Security Information -- DSA-3565-1 botan1.10	DEBIAN	www.debian.org	
Botan: Multiple vulnerabilities (GLSA 201701-23) — Gentoo security	GENTOO	security.gentoo.org	
'[botan-devel] Botan 1.10.13 released' - MARC	MLIST	marc.info	Vendor Advisory
Security — Botan	CONFIRM	botan.randombit.net	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710456 Gentoo Linux Botan Multiple Vulnerabilities (GLSA 201701-23)