



# CVE-2016-2849

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

## Summary

<b>CVE</b>	CVE-2016-2849
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-05-13 14:59:00 UTC
<b>Updated</b>	2017-07-01 01:29:00 UTC
<b>Description</b>	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	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.10.12	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.0	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.1	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.10	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.11	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.12	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.13	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.14	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.15	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.16	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.17	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.18	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.19	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.2	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.20	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.21	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	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	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.28	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.3	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.4	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.5	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.6	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.7	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.8	All	All	All
Application	<a href="#">Botan Project</a>	<a href="#">Botan</a>	1.11.9	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All

## References

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

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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