



CVE-2021-40529

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

Summary

CVE	CVE-2021-40529
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-06 19:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	The ElGamal implementation in Botan through 2.18.1, as used in Thunderbird and other products, allows plaintext recovery

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Botan Project	Botan	All	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

References

Reference	Source	Link
Cryptology ePrint Archive: Report 2021/923 - On the (in)security of ElGamal in OpenPGP	MISC	eprint.iacr.org
Avoid using short exponents with ElGamal by randombit · Pull Request #2790 · randombit/botan · GitHub	MISC	github.com
On the (in)security of ElGamal in OpenPGP - Part II - Syssec@IBM Research	MISC	ibm.github.io
Mozilla Thunderbird: Multiple Vulnerabilities (GLSA 202208-14) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 34 Update: botan2-2.17.3-4.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
On the (in)security of ElGamal in OpenPGP - Part I - Syssec@IBM Research	MISC	ibm.github.io
[SECURITY] Fedora 35 Update: botan2-2.18.2-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 34 Update: botan2-2.17.3-4.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 35 Update: botan2-2.18.2-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181906	Debian Security Update for botan (CVE-2021-40529)
282059	Fedora Security Update for botan2 (FEDORA-2021-8d51cac49f)
501731	Alpine Linux Security Update for botan
501949	Alpine Linux Security Update for botan
503874	Alpine Linux Security Update for botan
710585	Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 202208-14)
751542	OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2021:4150-1)
751566	OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2021:1635-1)

© [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](#)