CVE-2017-17688

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-17688
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-16 19:29:00 UTC
Updated	2023-11-07 02:41:00 UTC
Description	** DISPUTED ** The OpenPGP specification allows a Cipher Feedback Mode (CFB) malleability-gadget attack that can ind

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Mail	-	All	All	All
Application	Apple	Mail	-	All	All	All
Application	Apple	Mail	-	All	All	All
Application	Apple	Mail	-	All	All	All
Application	Bloop	Airmail	-	All	All	All
Application	Bloop	Airmail	-	All	All	All
Application	Emclient	Emclient	-	All	All	All
Application	Emclient	Emclient	-	All	All	All
Application	Flipdogsolutions	Maildroid	-	All	All	All
Application	Flipdogsolutions	Maildroid	-	All	All	All
Application	Freron	Mailmate	-	All	All	All
Application	Freron	Mailmate	-	All	All	All
Application	Horde	Horde Imp	-	All	All	All
Application	Horde	Horde Imp	-	All	All	All
Application	Microsoft	Outlook	2007	All	All	All
Application	Microsoft	Outlook	2007	All	All	All
Application	Mozilla	Thunderbird	-	All	All	All

Application	Mozilla	Thunderbird	-	All	All	All
Application	Postbox-inc	Postbox	-	All	All	All
Application	Postbox-inc	Postbox	-	All	All	All
Application	R2mail2	R2mail2	-	All	All	All
Application	R2mail2	R2mail2	-	All	All	All
Application	Roundcube	Webmail	-	All	All	All
Application	Roundcube	Webmail	-	All	All	All

References

Reference
A Unified Timeline
OpenPGP CFB Mode Authentication Flaw Lets Remote Users Decrypt and Obtain Potentially Sensitive Information from the Target User's Em
EFAIL
Cybersecurity Roundup: May 15, 2018 | Violet Blue on Patreon
Matthew Green na Twitterze: "So in summary, PGP clients are vulnerable because 17 years after a vulnerability was known, the mitigation wa
No, PGP is not broken, not even with the Efail vulnerabilities - ProtonMail Blog
Let's summarize the situation: Abstract: S/MIME and MUAs are broken. OpenPGP (... | Hacker News
Synology Inc.
OpenPGP CVE-2017-17688 Man In The Middle Information Disclosure Vulnerability
Efail press release
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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