CVE-2017-17689

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-17689
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-16 19:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The S/MIME specification allows a Cipher Block Chaining (CBC) malleability-gadget attack that can indirectly lead to plainte

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	9folders	Nine	-	All	All	All
Application	9folders	Nine	-	All	All	All
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	Gnome	Evolution	-	All	All	All
Application	Gnome	Evolution	-	All	All	All
Application	Google	Gmail	-	All	All	All

Application	Google	Gmail	-	All	All	All
Application	Horde	Horde Imp	-	All	All	All
Application	Horde	Horde Imp	-	All	All	All
Application	Ibm	Notes	-	All	All	All
Application	Ibm	Notes	-	All	All	All
Application	Kde	Kmail	-	All	All	All
Application	Kde	Kmail	-	All	All	All
Application	Kde	Trojita	-	All	All	All
Application	Kde	Trojita	-	All	All	All
Application	Microsoft	Outlook	2007	All	All	All
Application	Microsoft	Outlook	2010	All	All	All
Application	Microsoft	Outlook	2013	All	All	All
Application	Microsoft	Outlook	2016	All	All	All
Application	Microsoft	Outlook	2007	All	All	All
Application	Microsoft	Outlook	2010	All	All	All
Application	Microsoft	Outlook	2013	All	All	All
Application	Microsoft	Outlook	2016	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	Ritlabs	The Bat	-	All	All	All
Application	Ritlabs	The Bat	-	All	All	All

References

Reference
EFAIL
Multiple Products S/MIME CVE-2017-17689 Man In The Middle Information Disclosure Vulnerability
Matthew Green na Twitterze: "Someone asked me to summarize my views on the Efail matter, and the “controversy” in the PGP community. I
My thoughts about Efail are a bit more nuanced. First off, the real story her - Pastebin.com
Let's summarize the situation: Abstract: S/MIME and MUAs are broken. OpenPGP (... | Hacker News
Synology Inc.
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.