

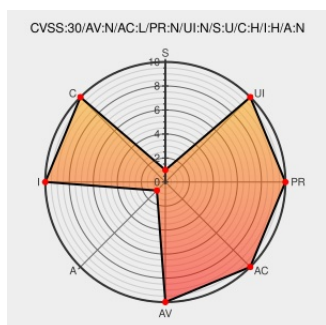


CVE-2018-6596

Published on: 02/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6596

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

webhooks/base.py in Anymail (aka django-anymail) before 1.2.1 is prone to a timing attack vulnerability on the WEBHOOK_AUTHORIZATION secret, which allows remote attackers to post arbitrary e-mail tracking events.

CVE-2018-6596 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: **6.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Release v1.2.1 · anymail/django-anymail · GitHub	Release Notes github.com text/html	CONFIRM github.com/anymail/django-anymail/releases/tag/v1.2.1
Release v1.3 · anymail/django-anymail · GitHub	Release Notes	CONFIRM github.com/anymail/django-

github.com

text/html

anymail/releases/tag/v1.3

Security: prevent timing attack on WEBHOOK_AUTHORIZATION secret · anymail/django-anymail@c079983 · GitHub

Patch

github.com

text/html

 **CONFIRM** github.com/anymail/django-anymail/commit/c07998304b4a31df4c61deddc03d3607a04691b

Debian -- Security Information -- DSA-4107-1
django-anymail

Third Party Advisory

www.debian.org

Deprecated Link

text/html

 **DEBIAN DSA-4107**

Security: prevent timing attack on WEBHOOK_AUTHORIZATION secret · anymail/django-anymail@db586ed · GitHub

Patch

github.com

text/html

 **CONFIRM** github.com/anymail/django-anymail/commit/db586ede1fbb41dce21310ea28ae15a1cf1286c5

#889450 - django-anymail: CVE-2018-6596: Security issue with timing attack on WEBHOOK_AUTHORIZATION - Debian Bug report logs

Issue Tracking

Patch

Third Party Advisory

bugs.debian.org

text/html

 **CONFIRM** bugs.debian.org/889450

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

981031 Python (pip) Security Update for django-anymail (GHSA-hxf9-7h4c-f5jv)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Django-anymail Project	Django-anymail	All	All	All	All
Application	Django-anymail Project	Django-anymail	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:django-anymail_project:django-anymail:*:*:*:*:*:						
cpe:2.3:a:django-anymail_project:django-anymail:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#)