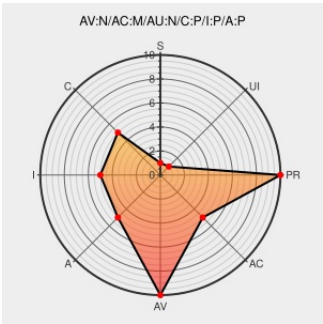
CVE-2014-3556

Published on: 12/29/2014 12:00:00 AM UTC

Last Modified on: 11/10/2021 03:59:00 PM UTC

CVE-2014-3556

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nginx from F5 contain the following vulnerability:

The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.

CVE-2014-3556 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Bug 1126891 – CVE-2014-3556 nginx: SMTP STARTTLS plaintext injection flaw	Issue Tracking, Third Party Advisory, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1126891
[nginx-announce] nginx security advisory (CVE-2014-3556)	Patch, Vendor Advisory, mailman.nginx.org, text/html	MLIST [nginx-announce] 20140805 nginx security advisory (CVE-2014-3556)
	Patch, Vendor Advisory, nginx.org	CONFIRM nginx.org/download/patch.2014.starttls.txt

	text/x-diff	
'[security bulletin] HPSBOV03227 rev.1 - HP SSL for OpenVMS, Remote Disclosure of Information, Denial' - MARC	Issue Tracking Third Party Advisory marc.info text/html	HP HPSBOV03227

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All

cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*:

cpe:2.3:a:nginx:nginx:*:*:*:*:*:*:*:*:

cpe:2.3:a:nginx:nginx:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→