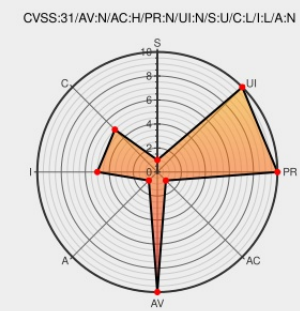
CVE-2020-5865

Published on: 04/23/2020 12:00:00 AM UTC

Last Modified on: 04/26/2022 05:16:00 PM UTC

CVE-2020-5865

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



Certain versions of Nginx Controller from F5 contain the following vulnerability:

In versions prior to 3.3.0, the NGINX Controller is configured to communicate with its Postgres database server over unencrypted channels, making the communicated data vulnerable to interception via man-in-the-middle (MiTM) attacks.

CVE-2020-5865 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	Vendor Advisory support.f5.com text/html	CONFIRM support.f5.com/csp/article/K21009022
April 2020 NGINX Vulnerabilities in NetApp Products | NetApp	security.netapp.com	CONFIRM security.netapp.com/advisory/ntap-

Product Security	text/html	20200430-0005/

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 Controller	All	All	All	All
Application	F5	Nginx Controller	1.0.1	All	All	All
Application	F5	Nginx Controller	All	All	All	All
Application	F5	Nginx Controller	1.0.1	All	All	All
Application	F5	Nginx Controller	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All

cpe:2.3:a:f5:nginx_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:nginx_controller:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:nginx_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:f5:nginx_controller:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:nginx_controller:*:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:cloud_backup:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | In versions prior to 3.3.0, the NGINX Co... | CVE-2020-5865 | Link for more: alerts.remotelyrmm.com/CVE-2020-5865	2022-04-26 18:29:22
@LinInfoSec	Nginx - CVE-2020-5865: support.f5.com/csp/article/K2…	2022-04-26 19:06:55

← Previous ID Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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