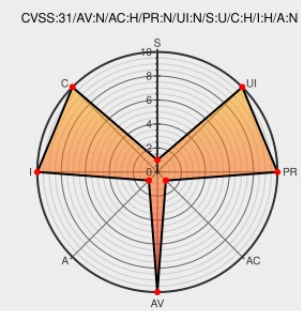
CVE-2020-5864

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

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5864

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



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

In versions of NGINX Controller prior to 3.2.0, communication between NGINX Controller and NGINX Plus instances skip TLS verification by default.

CVE-2020-5864 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.4 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	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/K27205552
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

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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→