CVE-2020-5867

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-5867
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-23 20:15:00 UTC
Updated	2022-04-26 17:22:00 UTC
Description	In versions prior to 3.3.0, the NGINX Controller Agent installer script 'install.sh' uses HTTP instead of HTTPS to check and i

Risk And Classification

Problem Types: CWE-319 | CWE-494

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
April 2020 NGINX Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
support.f5.com/csp/article/K00958787	CONFIRM	support.f5.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.