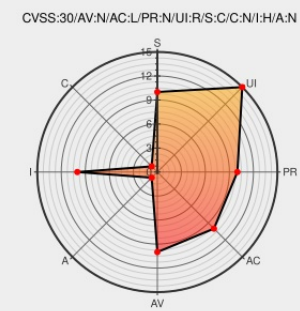
CVE-2017-6130

Published on: 04/06/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:49 PM UTC

CVE-2017-6130

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



Certain versions of Ssl Intercept Iapp from F5 contain the following vulnerability:

F5 SSL Intercept iApp 1.5.0 - 1.5.7 and SSL Orchestrator 2.0 is vulnerable to a Server-Side Request Forgery (SSRF) attack when deployed using the Dynamic Domain Bypass (DDB) feature feature plus SNAT Auto Map option for egress traffic.

CVE-2017-6130 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **F5 Networks** - **SSL Intercept iApp 1.5.0 - 1.5.7 and SSL Orchestrator 2.0** version **SSL Intercept iApp 1.5.0 - 1.5.7 and SSL Orchestrator 2.0**

CVSS3 Score: 7.4 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	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	CONFIRM support.f5.com/csp/article/K23001529

text/html

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	Ssl Intercept Iapp	1.5.0	All	All	All
Application	F5	Ssl Intercept Iapp	1.5.7	All	All	All
Application	F5	Ssl Intercept Iapp	1.5.0	All	All	All
Application	F5	Ssl Intercept Iapp	1.5.7	All	All	All
Application	F5	Ssl Orchestrator	2.0	All	All	All
Application	F5	Ssl Orchestrator	2.0	All	All	All

cpe:2.3:a:f5:ssl_intercept_iapp:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:ssl_intercept_iapp:1.5.7:*:*:*:*:*:*:*:

cpe:2.3:a:f5:ssl_intercept_iapp:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:ssl_intercept_iapp:1.5.7:*:*:*:*:*:*:*:

cpe:2.3:a:f5:ssl_orchestrator:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:ssl_orchestrator:2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→