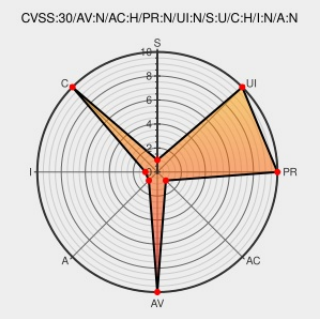
CVE-2018-7110

Published on: 10/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

CVE-2018-7110

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



Certain versions of Service Governance Framework from Hpe contain the following vulnerability:

A remote unauthorized disclosure of information vulnerability was identified in HPE Service Governance Framework (SGF) version 4.2, 4.3. A race condition under high load in SGF exists where SGF transferred different parameter to the enabler.

CVE-2018-7110 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Hewlett Packard Enterprise** - **HPE Service Governance Framework (SGF)** version **SGF v4.2,4.3**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Document Display | HPE Support Center	Vendor Advisory, support.hpe.com, text/html	CONFIRM support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03890en_us

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	Hpe	Service Governance Framework	4.2	All	All	All
Application	Hpe	Service Governance Framework	4.3	All	All	All
Application	Hpe	Service Governance Framework	4.2	All	All	All
Application	Hpe	Service Governance Framework	4.3	All	All	All
Operating System	Redhat	Linux	6.0	All	All	All
Operating System	Redhat	Linux	7.0	All	All	All
Operating System	Redhat	Linux	6.0	All	All	All
Operating System	Redhat	Linux	7.0	All	All	All

cpe:2.3:a:hpe:service_governance_framework:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:hpe:service_governance_framework:4.3:*:*:*:*:*:*:*:

cpe:2.3:a:hpe:service_governance_framework:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:hpe:service_governance_framework:4.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report