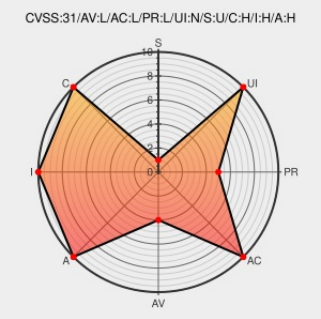
CVE-2020-7135

Published on: 04/27/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-7135

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



Certain versions of Service Pack For Proliant from Hp contain the following vulnerability:

A potential security vulnerability has been identified in the disk drive firmware installers named Supplemental Update / Online ROM Flash Component on HPE servers running Linux. The vulnerable software is included in the HPE Service Pack for ProLiant (SPP) releases 2018.06.0, 2018.09.0, and 2018.11.0. The vulnerable software is the Supplemental Update / Online ROM Flash Component for Linux (x64) software. The installer in this software component could be locally exploited to execute arbitrary code. Drive Models can be found in the Vulnerability Resolution field of the security bulletin. The 2019_03 SPP and Supplemental update / Online ROM Flash Component for Linux (x64) after 2019.03.0 has fixed this issue.

CVE-2020-7135 has been assigned by security-alert@hpe.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

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-hpesbhf03945en_us

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Service Pack For Proliant	2018.06.0	All	All	All
Application	Hp	Service Pack For Proliant	2018.09.0	All	All	All
Application	Hp	Service Pack For Proliant	2018.11.0	All	All	All
Application	Hp	Service Pack For Proliant	2019.03.0	All	All	All
Application	Hp	Service Pack For Proliant	2018.06.0	All	All	All
Application	Hp	Service Pack For Proliant	2018.09.0	All	All	All
Application	Hp	Service Pack For Proliant	2018.11.0	All	All	All
Application	Hp	Service Pack For Proliant	2019.03.0	All	All	All

cpe:2.3:a:hp:service_pack_for_proliant:2018.06.0:*:*:*:*:*:*:*:

cpe:2.3:a:hp:service_pack_for_proliant:2018.09.0:*:*:*:*:*:*:*:

cpe:2.3:a:hp:service_pack_for_proliant:2018.11.0:*:*:*:*:*:*:*:

cpe:2.3:a:hp:service_pack_for_proliant:2019.03.0:*:*:*:*:*:*:*:

cpe:2.3:a:hp:service_pack_for_proliant:2018.06.0:*:*:*:*:*:*:*:

cpe:2.3:a:hp:service_pack_for_proliant:2018.09.0:*:*:*:*:*:*:*:

cpe:2.3:a:hp:service_pack_for_proliant:2018.11.0:*:*:*:*:*:*:*:

cpe:2.3:a:hp:service_pack_for_proliant:2019.03.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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