

# SUPPORT COMMUNICATION - SECURITY BULLETIN

**Document ID:** hpesbhf03751en\_us

**Version:** 1

**HPESBHF03751 rev.1 - HPE Aruba AirWave Glass, Remote Code Execution**

**NOTICE:** The information in this Security Bulletin should be acted upon as soon as possible.

**Release Date:** 2017-05-24

**Last Updated:** 2017-05-24

---

**Potential Security Impact:** Remote: Code Execution

**Source:** Hewlett Packard Enterprise, HPE Software Security Response Team

## VULNERABILITY SUMMARY

A potential vulnerability in HPE Aruba AirWave Glass 1.0.0 and 1.0.1 could be remotely exploited to allow remote code execution.

## References:

- CVE-2017-8946 - remote code execution

## SUPPORTED SOFTWARE VERSIONS\*: ONLY impacted versions are listed.

- Aruba Airwave Software Glass v1.0.0 and 1.0.1 - Only AirWave Glass is affected; standard AirWave is not

## BACKGROUND

For a PGP signed version of this security bulletin please write to: [security-alert@hpe.com](mailto:security-alert@hpe.com)

CVSS Version 3.0 and Version 2.0 Base Metrics

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2017-8946	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:H	7.5	(AV:N/AC:H/Au:N/C:P/I:P/A:C)	6.8

Information on CVSS is documented in HPE Customer Notice: [HPSN-2008-002](#)

## RESOLUTION

HPE Aruba has provided the resolution to the vulnerability in AirWave Glass version 1.0.1-1.

A new OVA file is available from <https://support.arubanetworks.com>, or the system may be upgraded within the application through the administrative interface. Because an existing compromise may be difficult to detect, **Aruba strongly recommends downloading the OVA file and deploying a fresh installation of the product.**

**Note:** Please contact product support for questions about this resolution.

## HISTORY

Version:1 (rev.1) - 24 May 2017 Initial release

**Third Party Security Patches:** Third party security patches that are to be installed on systems running Hewlett Packard Enterprise (HPE) software products should be applied in accordance with the customer's patch management policy.

**Support:** For issues about implementing the recommendations of this Security Bulletin, contact normal HPE Services support channel. For other issues about the content of this Security Bulletin, send e-mail to [security-alert@hpe.com](mailto:security-alert@hpe.com).

**Report:** To report a potential security vulnerability for any HPE supported product:

- Web Form: <https://www.hpe.com/info/report-security-vulnerability>
- Email: [security-alert@hpe.com](mailto:security-alert@hpe.com)

**Subscribe:** To initiate a subscription to receive future HPE Security Bulletin alerts via Email: [http://www.hpe.com/support/Subscriber\\_Choice](http://www.hpe.com/support/Subscriber_Choice)

**Security Bulletin Archive:** A list of recently released Security Bulletins is available here: [http://www.hpe.com/support/Security\\_Bulletin\\_Archive](http://www.hpe.com/support/Security_Bulletin_Archive)

**Software Product Category:** The Software Product Category is represented in the title by the two characters following HPSB.

3C = 3COM

3P = 3rd Party Software

GN = HP General Software

HF = HP Hardware and Firmware

MU = Multi-Platform Software

NS = NonStop Servers

OV = OpenVMS

PV = ProCurve

ST = Storage Software

UX = HP-UX