SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: hpesbhf03730en_us
Version: 1
HPESBHF03730 rev.1 - HPE Aruba ClearPass Policy Manager, Mulitple Vulnerabilities

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: Access Restriction Bypass, Arbitrary Command Execution, Cross-Site Scripting (XSS), Disclosure of Information, Escalation of Privilege
Source: Hewlett Packard Enterprise, HPE Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified in HPE Aruba ClearPass Policy Manager. The vulnerabilities could be remotely exploited to allow access restriction bypass, arbitrary command execution, cross site scripting (XSS), escalation of privilege and disclosure of information.

References:

- CVE-2017-5824 - unauthenticated remote Code Execution
- CVE-2017-5825 - privilege escalation
- CVE-2017-5826 - authenticated Remote Code Execution
- CVE-2017-5827 - reflected XSS
- CVE-2017-5828 - arbitrary command execution via Xml External entity (XXE)
- CVE-2017-5829 - access restriction bypass
- CVE-2017-5647 - Apache Tomcat, information disclosure

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

- Aruba ClearPass Enterprise Software - All ClearPass Policy Manager versions prior to v6.6.5

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hpe.comb

CVSS Version 3.0 and Version 2.0 Base Metrics

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2017-5647	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2017-5824	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2017-5825	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L	5.0	(AV:N/AC:H/Au:S/C:P/I:P/A:P)	4.6
CVE-2017-5826	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L	5.0	(AV:N/AC:H/Au:S/C:P/I:P/A:P)	4.6
CVE-2017-5827	CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L	4.6	(AV:N/AC:H/Au:S/C:P/I:P/A:P)	4.6
CVE-2017-5828	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N	4.2	(AV:N/AC:H/Au:S/C:P/I:P/A:N)	3.6
CVE-2017-5829	CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N	3.6	(AV:L/AC:H/Au:N/C:P/I:P/A:N)	2.6

Information on CVSS is documented in HPE Customer Notice: HPSN-2008-002
Hewlett Packard Enterprise would like to thank the following researchers for reporting issues to security-alert@hpe.com:

- Luke Young (@TheBoredEng) for reporting CVE-2017-5824 through the BugCrowd managed bug bounty program.
- Luke Young (@TheBoredEng) for reporting CVE-2017-5825 through the BugCrowd managed bug bounty program.
- "fmast" for reporting CVE-2017-5826 through the BugCrowd BugCrowd managed bug bounty program.
- Phil Purviance (@superevr) of Bishop Fox for reporting CVE-2017-5827.
- V. Harishkumar (@harishkumar0394) for reporting CVE-2017-5828 through the BugCrowd managed bug bounty program.
- Luke Young (@TheBoredEng) for reporting CVE-2017-5829 through the BugCrowd managed bug bounty program.

RESOLUTION
HPE Aruba has provided the following resolution - Upgrade to ClearPass Policy Manager version 6.6.5 and then apply an additional hotfix. ClearPass 6.6.5 was released on March 30, 2017 and an updated version was released April 12, 2017. The additional hotfix is applicable to both versions of ClearPass 6.6.5 and was released on May 24, 2017. All future releases of ClearPass will include these fixes when released.

Installing the Patch Online Using the Software Updates Portal:

1. Open ClearPass Policy Manager and go to Administration > Agents and Software Updates > Software Updates.

2. In the Firmware and Patch Updates area, find the "ClearPass Cumulative Patch 5 for 6.6.0, 6.6.1, 6.6.2, 6.6.3 and 6.6.4" and click the Download button in its row.
3. Click Install.
4. When the installation is complete and the status is shown as "Needs Restart", proceed to restart ClearPass. After reboot, the status for the patch will be shown as Installed in Administration > Agents and Software Updates > Software Updates page.
5. While in the Firmware and Patch Updates area, find the "ClearPass 6.6.5 Hotfix Patch for CVE-2017-5647, CVE-2017-5824, and CVE-2017-5829" and click the Download button in its row.
6. Click Install.
7. When the installation is complete and the status is shown as "Needs Restart", proceed to restart ClearPass. After reboot, the status for the patch will be shown as Installed. The ClearPass Policy Manager version number will not change.

Installing the Patch Offline Using the Patch File from https://support.arubanetworks.com:

1. Download the "6.6.0 Cumulative Patch 5 (6.6.5)" and "ClearPass 6.6.5 Hotfix Patch for CVE-2017-5647, CVE-2017-5824, and CVE-2017-5829" from the Support site.
2. Open the ClearPass Policy Manager Admin UI and go to Administration > Agents and Software Updates > Software Updates.
3. At the bottom of the Firmware and Patch Updates area, click Import Updates and browse to the downloaded "6.6.0 Cumulative Patch 5 (6.6.5)" file.
4. Click Install.
8. When the installation is complete and the status is shown as Needs Restart, proceed to restart ClearPass. After reboot, the status for the patch will be shown as Installed in Administration > Agents and Software Updates > Software Updates page.
5. At the bottom of the Firmware and Patch Updates area, click Import Updates and browse to the downloaded " ClearPass 6.6.5 Hotfix Patch for CVE-2017-5647, CVE-2017-5824, and CVE-2017-5829)" file.
9. Click Install.
10. When the installation is complete and the status is shown as "Needs Restart", proceed to restart ClearPass. After reboot, the status for the patch will be shown as Installed. The ClearPass Policy Manager version number will not change.

Notes:

- **Temporary Mitigation:** These attacks require network access to execute. As a general best practice it is recommended that all administrative access be restricted to trusted user networks exclusively. This applies to the Policy Manager Admin Web Interface and SSH consoles. This is best accomplished through a comprehensive network security policy that restricts administrative access to ClearPass administration interfaces.
    - Restricting access to the Policy Manager Admin Web Interface can be accomplished by navigating to Administration >> Server Manager >> Server Configuration >> <Server-Name> >> Network >> Restrict Access and only allowing non-public or network management networks.
- Please contact HPE Aruba Technical Support if any assistance is needed.

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.

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

Subscribe: To initiate a subscription to receive future HPE Security Bulletin alerts via Email: 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

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

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