

Multiple Vulnerabilities in HPE Networking ClearPass Policy Manager



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	178
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-12
Issue Date	2026-10-06

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Multiple security vulnerabilities have been disclosed in HPE Networking ClearPass Policy Manager (formerly Aruba ClearPass Policy Manager).

The disclosed issues include remote code execution, authentication bypass, authorization bypass, privilege escalation, improper access control, SQL injection, path traversal, command injection, buffer overflow, denial-of-service (DoS), information disclosure, deserialization of untrusted data, missing integrity verification, and format string vulnerabilities. The most severe vulnerability carries a CVSS score of 9.9.

Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, escalate privileges, gain unauthorized access, perform SQL injection attacks, execute arbitrary commands, access or modify sensitive information, disrupt service availability, or otherwise compromise affected systems.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

CVE ID	Description
CVE-2026-79798 CVSS Score: 9.9	SQL injection vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow a low-privileged authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. Successful exploitation could allow an attacker to run arbitrary database commands.
CVE-2026-76750 CVSS Score: 9.8	Deserialization of untrusted data vulnerabilities exist in the web interface of HPE Networking ClearPass Policy Manager. Successful exploitation could allow an unauthenticated remote attacker to execute arbitrary code on the affected system.

CVE-2026-76751 CVSS Score: 9.8	A missing integrity verification vulnerability exists in the OnGuard agent of ClearPass Policy Manager. Successful exploitation could allow an unauthenticated, remote attacker to execute arbitrary code on the affected endpoint with the elevated privileges of the agent.
CVE-2026-76752 CVSS Score: 9.8	Authentication bypass vulnerabilities exist in the web-based management and API interfaces of HPE Networking ClearPass Policy Manager. Successful exploitation could allow an unauthenticated remote attacker to circumvent existing authentication controls and gain administrative access to the affected system.
CVE-2026-76753 CVSS Score: 9.8	A format string vulnerability in an affected service interface of HPE Networking ClearPass Policy Manager could allow an unauthenticated remote attacker to corrupt process memory. Successful exploitation could allow an attacker to execute arbitrary code.
CVE-2026-76754 CVSS Score: 9.8	A vulnerability in an affected interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. Successful exploitation could allow an attacker to run arbitrary database commands.
CVE-2026-79796 CVSS Score: 9.8	Vulnerabilities have been identified in the affected interface of ClearPass Policy Manager that could potentially allow an unauthenticated remote attacker to circumvent existing authentication controls. Successful exploitation could allow an attacker to gain unauthorized access to the affected system.
CVE-2026-79801 CVSS Score: 9.8	A missing integrity verification vulnerability in the client agent software of HPE Networking ClearPass Policy Manager could allow an unauthenticated remote attacker to introduce untrusted code. Successful exploitation could allow an attacker to execute arbitrary code on the affected client system.
CVE-2026-79805 CVSS Score: 9.8	An authenticated path traversal vulnerability exists in ClearPass Policy Manager. Successful exploitation could allow an attacker to read and modify certain files on the underlying operating system.
CVE-2026-79794 CVSS Score: 9.1	A SQL injection vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. Successful exploitation could allow an attacker to run arbitrary database commands.
CVE-2026-79797 CVSS Score: 8.8	An improper access control vulnerability exists in the Android client application for HPE Networking ClearPass Policy Manager, where application functionality may be invoked by untrusted sources. Successful exploitation could allow an unauthenticated remote attacker, with user interaction, to obtain sensitive information from the affected user.
CVE-2026-79799 CVSS Score: 8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.

CVE-2026-79800 CVSS Score: 8.8	An authenticated path traversal vulnerability exists in the command line interface of ClearPass Policy Manager. Successful exploitation could allow a low-privileged authenticated remote attacker to execute arbitrary code with elevated privileges on the underlying operating system.
CVE-2026-79802 CVSS Score: 8.8	A command injection vulnerability exists in the client software of ClearPass Policy Manager. Successful exploitation could allow an attacker who is able to supply crafted input to the affected software to execute arbitrary commands with elevated privileges on the affected host.
CVE-2026-79803 CVSS Score: 8.8	A command injection vulnerability exists in the API of ClearPass Policy Manager. Successful exploitation could allow an authenticated remote attacker to escalate privileges and gain administrative control of the affected system.
CVE-2026-79806 CVSS Score: 7.8	A privilege escalation vulnerability in the ClearPass Policy Manager OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges. A successful exploit allows a malicious user to escalate to root privileges on the affected Linux client.
CVE-2026-79807 CVSS Score: 7.8	A missing integrity verification vulnerability in the Windows client software for ClearPass Policy Manager could allow malicious users on a local instance to elevate their user privileges. A successful exploit could allow these users to execute attacker-supplied code with elevated privileges on the local system.
CVE-2026-79808 CVSS Score: 7.8	A buffer overflow vulnerability exists in the OnGuard agent of ClearPass Policy Manager. Successful exploitation could allow an authenticated local user to execute arbitrary code with elevated privileges on the affected host or to disrupt the availability of the affected service.
CVE-2026-79809 CVSS Score: 7.3	An unauthenticated path traversal vulnerability exists in an API endpoint of ClearPass Policy Manager. Successful exploitation of this vulnerability allows an unauthenticated remote attacker to influence authorization decisions and be assigned an unintended role.
CVE-2026-79810 CVSS Score: 7.2	Remote code execution vulnerabilities exist in the affected interface of HPE Networking ClearPass Policy Manager that could allow an authenticated remote attacker with high privileges to execute arbitrary code. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system.
CVE-2026-79811 CVSS Score: 7.2	A SQL injection vulnerability in the API of ClearPass Policy Manager could allow a remote authenticated attacker with administrative privileges to conduct SQL injection attacks against the ClearPass Policy Manager instance. Successful exploitation could allow an attacker to execute arbitrary database commands.
CVE-2026-79814 CVSS Score: 6.7	An arbitrary file write vulnerability in the ClearPass Policy Manager OnGuard agent could allow malicious users on a local instance to elevate their user privileges if certain preconditions outside of the attacker's control are met. Successful exploitation could allow a local attacker to execute arbitrary code with elevated privileges on the affected system.

CVE-2026-79813 CVSS Score: 6.7	A local privilege escalation vulnerability exists in the ClearPass client software. Successful exploitation could allow a low-privileged local user to execute commands with elevated privileges on the affected system, if certain conditions outside of the attacker's control are met.
CVE-2026-79815 CVSS Score: 6.5	A command injection vulnerability in the OnGuard agent of ClearPass Policy Manager could allow an authenticated remote attacker to inject arbitrary commands. Successful exploitation could allow an attacker to execute commands with elevated privileges on the affected Windows endpoint.
CVE-2026-79812 CVSS Score: 6.1	A denial-of-service vulnerability exists in the OnGuard agent of HPE Networking ClearPass Policy Manager. Successful exploitation could allow an authenticated local attacker to interrupt the normal operation of the agent service.
CVE-2026-79817 CVSS Score: 5.5	A sensitive information disclosure vulnerability exists in the client software of HPE Networking ClearPass Policy Manager. Successful exploitation could allow an attacker with local access to the affected system to obtain sensitive information.
CVE-2026-79816 CVSS Score: 5.4	A vulnerability in a client interface of HPE Networking ClearPass Policy Manager could allow an unauthenticated remote attacker to conduct a DOM-based cross-site scripting (XSS) attack against a user of the affected client interface. Successful exploitation could allow an attacker to execute arbitrary script code in a victim's browser context within the affected client interface.
CVE-2026-79818 CVSS Score: 5.3	A vulnerability in an API interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to circumvent existing authentication controls. Successful exploitation could allow an attacker to obtain sensitive information from the affected system.

Affected products

Product	Affected Version
HPE Networking ClearPass Policy Manager (CPPM)	CPPM 6.14.0 and below
	CPPM 6.11.15 and below

Recommendations

We recommend the following actions be taken:

- Apply appropriate updates, hot fixes or mitigations provided by HPE to vulnerable systems immediately after appropriate testing. ([M1051: Update Software](#))
 - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
 - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
 - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on

- a monthly, or more frequent, basis.
 - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
 - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
 - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
 - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
 - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
 - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic. (**M1037: Filter Network Traffic**)
 - **Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure:** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
 - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
 - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
 - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05158en_us&docLocale=en_US

CVE

CVE-2026-79798
CVE-2026-76750
CVE-2026-76751
CVE-2026-76752
CVE-2026-76753
CVE-2026-76754
CVE-2026-79796
CVE-2026-79801
CVE-2026-79805
CVE-2026-79794
CVE-2026-79797
CVE-2026-79799
CVE-2026-79800
CVE-2026-79802
CVE-2026-79803
CVE-2026-79806
CVE-2026-79807
CVE-2026-79808
CVE-2026-79809
CVE-2026-79810
CVE-2026-79811
CVE-2026-79814
CVE-2026-79813
CVE-2026-79815
CVE-2026-79812
CVE-2026-79817
CVE-2026-79816
CVE-2026-79818

