RealPresence Resource Manager 8.4 security fixes summary

June 29, 2015

On June 26, 2015 SEC Consult disclosed a set of vulnerabilities, applicable to Polycom RealPresence Resource Manager (RPRM) versions 8.3.2 and earlier.

https://packetstormsecurity.com/files/132463/Polycom-RealPresence-Resource-Manager-RPRM-Disclosure-Traversal.html

Of the nine vulnerabilities listed by SEC Consult, seven have been fixed in RPRM 8.4 and CVE numbers have been assigned (see below).

Two remaining vulnerabilities are exploitable only by users with administrator or auditor roles, and Polycom will be issuing an update to address these vulnerabilities in the near future.

RealPresence Resource Manager 8.4 is now available for customer download. Polycom recommends that all RPRM customers upgrade to version 8.4 as soon as possible. The 8.4 software update is available from the Polycom support web site and the following security issues:

CVE Identifier: CVE-2015-4681

Description:
Polycom RealPresence Resource Manager 8.3.2 and earlier contains instances of weak passwords.

"Polycom thanks Rene Freingruber from the SEC Consult Vulnerability Lab (https://www.sec-consult.com/) for responsibly reporting the identified issues."

CVSS v2 Base Score: 6.0 (AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVE Identifier: CVE-2015-4682

Description:

An absolute path disclosure vulnerability in Polycom RealPresence Resource Manager 8.3.2 and earlier allows an attacker to see the path to the webroot. This information leakage can be used to refine attacks against the webserver.

"Polycom thanks Rene Freingruber from the SEC Consult Vulnerability Lab (https://www.sec-consult.com/) for responsibly reporting the identified issues."

CVSS v2 Base Score: 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)

CVE Identifier: CVE-2015-4683

Description:
Polycom RealPresence Resource Manager 8.3.2 and earlier transmits session-IDs as a URL parameter, which can be used by an unprivileged attacker to gain admin-level privileges.

"Polycom thanks Rene Freingruber from the SEC Consult Vulnerability Lab (https://www.sec-consult.com/) for responsibly reporting the identified issues."

CVSS v2 Base Score: 5.2 (AV:A/AC:L/Au:S/C:P/I:P/A:P)

CVE Identifier: CVE-2015-4684

Description:
Polycom RealPresence Resource Manager 8.3.2 and earlier allow remote authenticated administrator users to read or write arbitrary files.

"Polycom thanks Rene Freingruber from the SEC Consult Vulnerability Lab (https://www.sec-consult.com/) for responsibly reporting the identified issues."

CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVE Identifier: CVE-2015-4685

Description:
Polycom RealPresence Resource Manager 8.3.2 and earlier contains a sudo misconfiguration that could allow an attacker to escalate their privileges.

"Polycom thanks Rene Freingruber from the SEC Consult Vulnerability Lab (https://www.sec-consult.com/) for responsibly reporting the identified issues."

CVSS v2 Base Score: 6.6 (AV:L/AC:M/Au:S/C:C/I:C/A:C)

Plaintext passwords stored in logfiles

SEC Consult describes this vulnerability as:

"RPRM generates logdata which includes plaintext passwords. This weakness in combination with the previous vulnerability allows an unprivileged attacker to escalate his privileges to the admin level in the web interface."

The "previous vulnerability" mentioned by SEC Consult has been fixed in RPRM 8.4. Only users with administrator or auditor role can read the affected logs.

Polycom is working on the issue and will soon release an update to address this.

Weak/Missing Authorization

SEC Consult describes this vulnerability as:

"The separation of users relies on the fact that conference IDs are not guessable, but as soon as an information disclosure vulnerability allows an attacker to gather conference IDs authorization can be bypassed. The arbitrary file download vulnerability (2) allows an attacker to collect valid conference IDs."

The "arbitrary file download vulnerability" mentioned by SEC Consult has been fixed in RPRM 8.4. Only users with an administrator or auditor role can read logfiles that contain valid conference IDs.

Polycom is working on the issue and will soon release an update to address this.