Proactive Notification: Advisory

June 14, 2018

CA Privileged Access Management customers, please review the following security notice.

All vulnerabilities listed in this notice below have been remediated. Please refer to the table in the Affected Products section of this notice for details.

For the latest version of this security notice, see

CA20180614-01: Security Notice for CA Privileged Access Manager

CA20180614-01: Security Notice for CA Privileged Access Manager

Issued: June 14, 2018
Last Updated: June 14, 2018

CA Technologies Support is alerting customers to multiple potential risks with CA Privileged Access Manager. Multiple vulnerabilities exist that can allow a remote attacker to conduct a variety of attacks. These risks include seven vulnerabilities privately reported within the past year to CA Technologies by security researchers, and nine vulnerabilities for Xceedium Xsuite that were publicly disclosed in July 2015. CA Technologies acquired Xceedium in August 2015, and Xceedium products were renamed and became part of Privileged Access Management solutions from CA Technologies.

The first vulnerability, CVE-2018-9021, has a high risk rating and concerns the ajax_cmd.php file, which can allow a remote attacker to execute arbitrary commands.

The second vulnerability, CVE-2018-9022, has a high risk rating and concerns configuration file poisoning, which can allow a remote attacker to execute arbitrary code.

The third vulnerability, CVE-2018-9023, has a medium risk rating and concerns the update_crld script, which can allow an unprivileged user to gain root privileges.

The fourth vulnerability, CVE-2018-9024, has a low risk rating and concerns IP spoofing in logs, which can allow a remote attacker to masquerade as another machine.

The fifth vulnerability, CVE-2018-9025, has a low risk rating and concerns insufficient input validation on the login page, which can allow a remote attacker to poison a log file.

The sixth vulnerability, CVE-2018-9026, has a medium risk rating and concerns insecure handling of user sessions in multiple scripts, which can allow a remote attacker to conduct session fixation attacks.

The seventh vulnerability, CVE-2018-9027, has a medium risk rating and concerns insufficient input validation in multiple scripts, which can allow a remote attacker to conduct reflected XSS attacks.

The eighth vulnerability, CVE-2015-4664, has a high risk rating and concerns insufficient input validation in the login.php script, which can allow a remote attacker to execute arbitrary commands.

The ninth vulnerability, CVE-2015-4665, has a medium risk rating and concerns insufficient input validation in the ajax_cmd.php script, which can allow a remote attacker to conduct reflected XSS attacks.

The tenth vulnerability, CVE-2015-4666, has a high risk rating and concerns insufficient input validation in the read_sessionlog.php script, which can allow an unauthenticated remote attacker to conduct directory traversal attacks and download sensitive information.

The eleventh vulnerability, also CVE-2015-4664, has a high risk rating and concerns insufficient input validation by the spadmind script, which can allow a local attacker to execute privileged commands.

The twelfth vulnerability, CVE-2015-4667, has a low risk rating and concerns the use of hard-coded credentials in multiple scripts, which can allow an attacker to potentially conduct a variety of attacks.

The thirteenth vulnerability, CVE-2015-4669, has a high risk rating and concerns insecure database credentials, which can allow a local user to conduct a variety of attacks.

The fourteenth vulnerability, CVE-2015-4668, has a low risk rating and concerns the openwin.php script, which can allow a remote attacker to conduct open redirect attacks.

The fifteenth vulnerability, CVE-2018-9028, has a low risk rating and concerns unsalted passwords, which can allow an attacker to more easily crack passwords.

The sixteenth vulnerability, CVE-2018-9029, has a medium risk rating and concerns insufficient input validation in multiple scripts, which can allow an attacker to conduct SQL injection attacks.

Risk Rating

See table in Affected Products section.

Platform(s)

All supported platforms

Affected Products

CVE	Risk Rating	Date Reported	Affected Versions	Versions Fixed	Fix Release Date
CVE-2018-9021	High	2017-05-08	2.8.2 and earlier	2.8.3, 3.0.0	2017-07-25
CVE-2018-9022	High	2017-05-22	2.8.2 and earlier	2.8.3, 3.0.0	2017-07-25
CVE-2018-9023	Medium	2017-05-19	2.x	3.0.0	2017-09-29
CVE-2018-9024	Low	2017-05-19	2.x	3.0.0	2017-09-29
CVE-2018-9025	Low	2017-05-19	2.x	3.0.0	2017-09-29
CVE-2018-9026	Medium	2017-05-19	2.x	3.0.0	2017-09-29
CVE-2018-9027	Medium	2017-05-19	2.x	3.0.0	2017-09-29
CVE-2015-4664	High	2015-07-22	2.4.4.4 and earlier	2.4.4.5	Before 2015-08-17
CVE-2015-4665	Medium	2015-07-22	2.4.4.1 and earlier	2.4.4.2	Before 2015-08-17
CVE-2015-4666	High	2015-07-22	2.4.4.5 and earlier	2.4.4.6	Before 2015-08-17
CVE-2015-4667	Low	2015-07-22	2.x	3.0.0	2017-09-29
CVE-2015-4669	High	2015-07-22	2.x	3.0.0	2017-09-29

CVE-2015-4668	Low	2015-07-22	2.4.4.5 and earlier	2.4.4.6	Before 2015-08-17
CVE-2018-9028	Low	2015-07-22	2.x	3.0.0	2017-09-29
CVE-2018-9029	Medium	2015-07-22	2.x	3.0.0	2017-09-29

Unaffected Products

CA Privileged Access Manager 3.0.0 or later

How to determine if the installation is affected

Customers may use the CA Privileged Access Manager interface to find the release and then use the table in the Affected Products section to determine if the installation is vulnerable.

Solution

CA Technologies published the following solution to address the vulnerabilities.

CA Privileged Access Manager:
Update to CA Privileged Access Manager 3.0.0 or later to address all vulnerabilities in this security notice.
CA Privileged Access Management support page

References

CVE-2018-9021 – PAM ajax_cmd.php RCE
CVE-2018-9022 – PAM configuration file poisoning RCE
CVE-2018-9023 – PAM update_crld privilege escalation
CVE-2018-9024 – PAM IP spoofing in logs
CVE-2018-9025 – PAM log poisoning
CVE-2018-9026 – PAM session fixation
CVE-2018-9027 – PAM reflected XSS
CVE-2015-4664 – PAM login.php RCE
CVE-2015-4665 – PAM ajax_cmd.php reflected XSS
CVE-2015-4666 – PAM read_sessionlog.php directory traversal
CVE-2015-4664 – PAM spadmind command execution
CVE-2015-4667 – PAM hard-coded credentials
CVE-2015-4669 – PAM insecure database credentials
CVE-2015-4668 – PAM openwin.php open redirect
CVE-2018-9028 – PAM unsalted passwords
CVE-2018-9029 – PAM SQL injection
Xceedium Is Now CA Technologies

Acknowledgement

CVE-2018-9021 – Peter Lapp
CVE-2018-9022 – Dan Cocking
CVE-2018-9023 – Peter Lapp
CVE-2018-9024 – Peter Lapp
CVE-2018-9025 – Peter Lapp
CVE-2018-9026 – Peter Lapp
CVE-2018-9027 – Peter Lapp

Change History

Version 1.0: 2018-06-14 - Initial Release

CA will send a notification about this security notice to customers who are subscribed to Proactive Notifications.

If additional information is required, please contact CA Technologies Support at http://support.ca.com/.

If you discover a vulnerability in a CA Technologies product, please send a report to the CA Technologies Product Vulnerability Response Team.

CA Technologies security notices