Proactive Notification: Advisory

January 13, 2016

To: Customers of CA Privileged Identity Manager
From: The CA Privileged Identity Manager Product Team
Subject: Windows 8.1, 2012 and 2012 R2 Endpoint Support

Recently, Microsoft has introduced changes to the Windows 8.1, 2012 and 2012 R2 operating systems that have impacted some of the capabilities provided in our agent-based software. While CA Privileged Identity Manager offers significant protection for Windows operation systems, the following features will no longer be supported:

For Windows 8.1, Windows 2012 and Windows 2012 R2 Operating Systems:

Stack Overflow Protection (STOP): Stack Overflow Protection (STOP) is a feature that prevents hackers from creating and exploiting stack overflow to break into systems. STOP works by intercepting crucial operating system calls to each application on the computer. Each call is then given an initial analysis before being sent for further analysis if it is seems suspicious. Further analysis is performed using data from the STOP configuration and signature files.

WINSERVICE Protection: A *Windows service* is a program that runs in the background on Windows, and is the Windows equivalent to a daemon on UNIX. The CA Privileged Identity Manager Windows service protection intercepts service access events that originate from one of the following:

Service management and information events.

Service database management events.

Configuration of Windows Batch files as program object: Protects Windows batch files (.bat) by ensuring that their contents or attributes haven’t been modified.

RunAs Application Protection: This prevents a user from impersonating another user's identity if they are not authorized to do so. CA Privileged Identity Manager intercepts impersonation requests that originate from the Windows RunAs utility.

Database/IIS/.NET integration: Protects against the use of hardcoded passwords in scripts and applications.

CA Privileged Identity Manager still provides significant protection for Windows operating systems including:

File protection

CA Privileged Identity Manager restricts a user's ability to access a file. You can give a user one or more types of access, such as READ, WRITE, EXECUTE, DELETE, and RENAME.

Terminals

CA Privileged Identity Manager performs checks to see if a is user authorized to use a particular terminal.

Sign-on time

Is a user authorized to log on at a particular time on a particular day?
Most users use their stations only on weekdays and only during work hours; the time-of-day and day-of-week login restrictions, as well as holiday restrictions, provide protection from hackers and from other unauthorized accessors.

TCP/IP

CA Privileged Identity Manager includes firewalls that prevent local stations and servers from providing services to unknown stations.

Multiple login privileges

CA Privileged Identity Manager can prevent a user from logging in more than once. This prevents intruders from logging into the accounts of users who are already logged in.

User-defined entities

You can define and protect both regular entities (such as TCP/IP services and terminals) and functional entities (known as *abstract*objects).

Aspects of administrator authority

CA Privileged Identity Manager provides the means to both delegate superuser authorities to operators and restrict the privilege of the superuser account.

Registry keys

CA Privileged Identity Manager restricts a user's ability to access registry keys. You can give a user one or more types of access, such as READ, WRITE, and DELETE. The access can be specified with regard to an individual registry key or to a set of similarly named registry keys.

Programs

The security administrator can test programs to ensure that they do not contain any security loopholes that can be used to gain unauthorized access. Programs that pass the test and are considered safe, are defined as trusted programs. The CA Privileged Identity Manager selfprotection module (also referred to as the **watchdog**) knows which program is in control at a particular time and checks whether the program has been modified or moved since it was classified as trusted. If a trusted program is modified or moved, the program is no longer considered trusted and CA Privileged Identity Manager does not allow it to run.

In addition, CA Privileged Identity Manager protects against various deliberate and accidental threats, including:

Kill attempts
CA Privileged Identity Manager can be used to protect critical servers and services or daemons against kill attempts.

Password Attack
CA Privileged Identity Manager protects against various types of password attacks, enforces the password-definition policies of your site, and detects break-in attempts.

Password Delinquency
CA Privileged Identity Manager policies delineate rules that force users to create and use passwords of sufficient quality. To ensure that users create and use acceptable passwords, CA Privileged Identity Manager can set maximum and minimum lifetimes for passwords, restrict certain words, prohibit repetitive characters, and enforce other restrictions. Passwords are not permitted to last too long.

Account Management
CA Privileged Identity Manager policies ensure that dormant accounts are dealt with appropriately.

If you have any questions regarding the support schedule, please contact CA Support at CA Support Online (https://support.ca.com/), your local CA Account Manager, Customer Success Manager or CA Customer Care online at http://www.ca.com/us/customer-care.aspx where you can submit an online request using the Customer Care web form: https://support.ca.com/irj/portal/anonymous/customercare. You can also call CA Customer Care at +1-800-225-5224 in North America or see http://www.ca.com/phone for the local number in your country.

Your success is very important to us, and we look forward to continuing our successful partnership with you.