SECURITY BULLETIN

Privilege Escalation Due To Weak ACLs

Bulletin Number
[20160125-1]

Issue Date
25 January 2016

CVE
[CVE-2015-7596]
[CVE-2015-7597]
[CVE-2015-7598]
[CVE-2015-7961]
[CVE-2015-7962]
[CVE-2015-7963]
[CVE-2015-7964]
[CVE-2015-7965]
[CVE-2015-7966]
[CVE-2015-7967]

Severity Level
Medium

Type
Local Privilege Escalation

Known Exploits
None

Mitigation Provided
Yes

Description

The installation of SafeNet Authentication Server agents is vulnerable to privilege escalation due to weak Access Control Lists (ACLs) assigned in some of the installation subdirectories and executable modules.

This vulnerability has been identified by NIST in the National Vulnerability Database under the Common Vulnerabilities and Exposures (CVE) numbers listed on the left. The National Vulnerability Database assessment of the vulnerability is not yet available as of the issue date of this Security Bulletin, but when they become available they can be found by searching under the appropriate CVE number:

https://web.nvd.nist.gov/view/vuln/search

Risk

This vulnerability allows any authenticated user from any user-group (guests included), to have full control over the contents of the Agent's file structure. As a result, a user from a limited account can substitute or modify some of the executable modules. As such, an executable module which requires Administrator privileges could be modified and executed by an Administrator, giving an attacker or imposter full access to the compromised host.

Products Impacted

The following products have been determined to have this vulnerability:

CVE	Product
[CVE-2015-7965] [CVE-2015-7966]	SafeNet Authentication Service Windows Logon Agent
[CVE-2015-7597]	SafeNet Authentication Service IIS Agent
[CVE-2015-7598]	SafeNet Authentication Service TokenValidator Proxy Agent
[CVE-2015-7962]	SafeNet Authentication Service for Outlook Web App Agent
[CVE-2015-7963]	SafeNet Authentication Service for AD FS Agent
[CVE-2015-7964]	SafeNet Authentication Service for NPS Agent
[CVE-2015-7961]	SafeNet Authentication Service Remote Web Workplace Agent
[CVE-2015-7967]	SafeNet Authentication Service for Citrix Web Interface Agent
[CVE-2015-7596]	SafeNet Authentication Service End User Software Tools for Windows

Mitigation

At the time of this issue date, most affected agents have a maintenance release available to address this issue. Maintenance releases are available on the SafeNet Authentication Service Downloads or via the Service Portal under the following document IDs:

Product	Document ID
SafeNet Authentication Service for Outlook Web App Agent	DOW4116
SafeNet Authentication Service for AD FS Agent	DOW4094
SafeNet Authentication Service for NPS Agent	DOW4117
SafeNet Authentication Service TokenValidator Proxy Agent	DOW4127

The following affected agents have a planned maintenance release that is not yet available at the time of this issue date. This Security Bulletin will be updated with Document IDs for these maintenance releases as they become available. As an interim solution, these products can follow the instructions for the manual mitigation process until the maintenance release is available. The expected released dates are provided in the table below.

Product	Maintenance Release Date
SafeNet Authentication Service IIS Agent	31 January 2016
SafeNet Authentication Service End User Software Tools for Windows	February 2016
SafeNet Authentication Service Windows Logon Agent	Q1, 2016

The following affected agents do not have a maintenance release scheduled. The vulnerability in these agents can be manually mitigated by the system administrator, as outlined below.

Product
SafeNet Authentication Service Remote Web Workplace Agent
SafeNet Authentication Service for Citrix Web Interface Agent

For these products, follow the manual process outlined below to modify the permissions in order to mitigate the vulnerability.

Instructions for Manual Mitigation by Modifying Permissions

1. Go to the agent’s local <installation folder>
2. Right-click on the <installation folder> → Properties → Security
3. Click on the Edit button and set the following:
   a. Authenticated Users: remove the full control/modify/write permissions. Allow Read & Execute only → Apply and Close
   b. Add Administrators group and allow full permissions list → Apply and Close
   c. Click Advance button and verify that all child objects inherits the new permission → Apply and Close