GE Digital Product Security Advisory

Title:	Proficy HMI/SCADA – CIMPLICITY Services DACLs
Vulnerability ID:	GED 16-01
Other identifiers:	CVE 2016-5787
Release date:	July 12, 2016
Last updated:	July 12, 2016

Summary

Discretionary Access Control Lists (DACLs) for Proficy HMI/SCADA – CIMPLICITY services enabled users to edit configuration of a service.

The issue, which affected CIMPLICITY 8.2 SIM 26 or earlier, was fully addressed by SIM27 in August 2014. The SIM from that time is available at:

https://ge-ip.force.com/communities/en_US/Download/CIMPLICITY-8-2-SIM-27-DN

GE Digital recommends that customers upgrade to Proficy HMI/SCADA – CIMPLICITY 8.2 SIM 27 or later or CIMPLICITY 9.0 and 9.5.

Proficy HMI/SCADA – CIMPLICITY customers unable to upgrade to version 8.2 SIM 27 or later are encouraged to consider the recommendations outlined in the "Other Recommendations" section of this document.

Affected software

Proficy HMI/SCADA – CIMPLICITY: Version 8.2 with SIM 26 and prior.

Solution

Fixes for this were released in CIMPLICITY 8.2 SIM 27. CIMPLICITY 9.0 AND 9.5 do not contain this issue.

The solution is to download the latest CIMPLICITY 8.2 SIM.

https://ge-ip.force.com/communities/en_US/Download/CIMPLICITY-8-2-SIM-43

Proficy SIMs are cumulative. All future SIMs will include these updates. The latest SIMs are available for download at http://support.ge-ip.com.

Other Recommendations

GE Digital recommends that all customers upgrade to the latest SIMs. Workaround may mitigate issues but only patches and SIMs will fully address an issue.

Edit the DACLs

- For version of CIMPLICITY prior to version 8.2 SIM 27, the service can be secured using the following commands from a command prompt.

```
sc sdset CIMPLICITY
D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWRPWPD
TLOCRRC;;;SU)(A;;CCLCSWRPWP;;;BU)

sc sdset WEBVIEW
D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWRPWPD
TLOCRRC;;;SU)


sc sdset "EGD Service"
D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)

sc sdset CimProxy
D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)
```

Vulnerability information

If the Discretionary Access Control Lists (DACLs) for Proficy HMI/SCADA – CIMPLICITY services remain unpatched or upgraded, any authenticated user on the system can modify the CIMPLICITY service to launch any executable on the system as a service. A CVSS v3 base score of 5.7 has been assigned; the CVSS vector string is (AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L).

Disclaimer

Change log

Date	Change(s)
07/08/16	• Initial release