MWR LABS

Security Advisory

SETUID bit set in OMNIRESOLVE

02/08/2017

Software	HPE Data Protector
Affected Versions	Prior to 8.17 and 9.09.
CVE Reference	CVE-2017-5809
Author	James Barlow-Bignell
Severity	Medium
Vendor	Hewlett Packard Enterprise
Vendor Response	Fix Released

Description:

The OMNIRESOLVE executable component of HPE Data Protector is installed by default with the SETUID bit set, and is owned by the root user. The executable does not check that the provided input files are valid, and logs verbose errors containing the file contents, and so it can be used to read files which the user does not have permission to access.

For example, the following command can be used to read the shadow file:

```
$ /opt/omni/lbin/omniresolve -i /etc/shadow
root:!:17105:0:99999:7:::
daemon:*:17001:0:99999:7:::
bin:*:17001:0:99999:7:::
sys:*:17001:0:99999:7:::
...
```

Impact:

This issue can be exploited by a local user to access sensitive files on the host, including password hashes and SSH keys, which could be used to elevate privileges and compromise other accounts.

Cause:

The SETUID bit is set by default on the OMNIRESOLVE executable, and the file is owned by the root user. The OMNIRESOLVE application is therefore able to read any file on the filesystem. As the program outputs the contents of its configuration file to the terminal if the configuration is found to be invalid, it is possible to read any arbitrary file by passing it to OMNIRESOLVE as the configuration file.

Solution:

A software update for HPE Data Protector is available from the vendor. HPE Data Protector should be updated to at least version 8.17 or 9.09 to resolve this issue.

Detailed Timeline

Date	Summary
02/12/2016	Issue reported to vendor.
13/01/2017	Issue confirmed by vendor.
02/08/2017	Vendor confirms fixes for versions 8.x and 9.x are available.