

# [VulnWatch] NSFOCUS SA2003-07: HP-UX Software Distributor Buffer Overflow Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-11/0010.html>

---

*From:* NSFOCUS Security Team ([security\\_at\\_nsfocus.com](mailto:security_at_nsfocus.com))

*Date:* 11/13/03

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

Date: Thu, 13 Nov 2003 17:40:48 +0800

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

NSFOCUS Security Advisory(SA2003-07)

Topic: HP-UX Software Distributor Buffer Overflow Vulnerability

Release Date: 2003-11-13

CVE CAN ID: CAN-2003-0089

<http://www.nsfocus.com/english/homepage/research/0307.htm>

Affected system:

=====

-- HP-UX B.11.00

-- HP-UX B.11.11

Summary:

=====

NSFOCUS Security Team has found a buffer overflow in Software Distributor utilities for HP-UX. By exploiting the vulnerability local attackers could gain root privilege.

Description:

=====

The Software Distributor(SD) utilities for HP-UX contain a number of programs such as swinstall. These programs are used to create, install, distribute and manage software products. A buffer overflow exists in the programs with suid root bit (such as swinstall/swmodify etc) and allows local attackers to run arbitrary code with root privilege.

## VulnWatch: [VulnWatch] NSFOCUS SA2003-07: HP-UX Software Distributor Buffer Overflow Vulnerability

If the environment variable LANG is set as a over large string, programs such as swinstall will copy it into a fixed-size buffer without any bound check, which causes a stack overflow. By overwriting the returned address and other data in the stack, local attackers could gain root privilege.

### Workaround:

=====

NSFOCUS suggests to temporarily remove the suid root bit for all the programs in SD utilities.

```
# chmod a-s /usr/sbin/sw*
```

### Vendor Status:

=====

2002.11.19 Informed the vendor

2002.12.05 Vendor confirmed the vulnerability

2003.11.05 Vendor released a security bulletin (HPSBUX0311-293) and relative patches for the vulnerability.

Detailed information for the HP security bulletin is available at:

<http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-293>

Note: Valid ITRC account is required for the link above.

### Patch ID:

HP-UX B.11.00 PHCO\_28847

HP-UX B.11.11 PHCO\_28848

### Additional Information:

=====

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-2003-0089 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems. Candidates may change significantly before they become official CVE entries.

### Acknowledgment

=====

Yang Jilong of NSFOCUS Security Team found the vulnerability.

### DISCLAIMS:

=====

THE INFORMATION PROVIDED IS RELEASED BY NSFOCUS "AS IS" WITHOUT WARRANTY OF ANY KIND. NSFOCUS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, EXCEPT FOR THE WARRANTIES OF MERCHANTABILITY. IN NO EVENT SHALL NSFOCUS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT,

INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES,  
EVEN IF NSFOCUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.  
DISTRIBUTION OR REPRODUCTION OF THE INFORMATION IS PROVIDED THAT THE  
ADVISORY IS NOT MODIFIED IN ANY WAY.

Copyright 1999-2003 NSFOCUS. All Rights Reserved. Terms of use.

NSFOCUS Security Team <security@nsfocus.com>  
NSFOCUS INFORMATION TECHNOLOGY CO.,LTD  
(<http://www.nsfocus.com>)

PGP Key: <http://www.nsfocus.com/homepage/research/pgpkey.asc>  
Key fingerprint = F8F2 F5D1 EF74 E08C 02FE 1B90 D7BF 7877 C6A6 F6DA  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQE/s1Gt1794d8am9toRAi9hAJ9ZDvJdiwPkgd1hSE9IquU06nts2wCfW0UJ  
9KQYdGocpQZhGHBHluB91IQ=  
=9nOm  
-----END PGP SIGNATURE-----