

# HP Propel

## Important Update for Linux® GHOST Vulnerability



**Software Versions: 1.00, 1.01, 1.10**

**Document Release Date: February 2015**

## Contents

<b>HP Propel Update for Linux GHOST Vulnerability.....</b>	<b>2</b>
Mitigation.....	2
Verify whether your HP Propel product is affected.....	2
Action to remove vulnerability .....	3

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Restricted rights legend: Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. AMD is a trademark of Advanced Micro Devices, Inc. Intel and Xeon are trademarks of Intel Corporation in the U.S. and other countries. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

## HP Propel Update for Linux GHOST Vulnerability

This **IMPORTANT UPDATE** is part of an HP Software Global Products Support program.

HP Propel 1.00, 1.01 and 1.10 can include impacted third-party applications (for example, web server or application servers) compromised by the Linux GHOST Vulnerability.

**We recommend that our customers refer to the mitigation provided below and follow the guidelines.**

Product name	Version(s)
HP Propel	1.00, 1.01, 1.10

### Mitigation

#### Verify whether your HP Propel product is affected

To test whether your version of glibc is vulnerable to GHOST, follow these steps:

1. Create a new file in Linux OS named ghost.c, and copy the following code into ghost.c.

```
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.h>
#include <gnu/libc-version.h>
#define CANARY "in_the_coal_mine"
struct {
char buffer[1024];
char canary[sizeof(CANARY)];
} temp = { "buffer", CANARY };
int main(void) {
struct hostent resbuf;
struct hostent *result;
int herrno;
int retval;
/**/ strlen (name) = size_needed - sizeof (*host_addr) - sizeof
(*h_addr_ptrs) - 1; /**/
size_t len = sizeof(temp.buffer) - 16*sizeof(unsigned char) -
2*sizeof(char *) - 1;
char name[sizeof(temp.buffer)];
memset(name, '0', len);
name[len] = '\0';
retval = gethostbyname_r(name, &resbuf, temp.buffer,
sizeof(temp.buffer), &result, &herrno);
if (strcmp(temp.canary, CANARY) != 0) {
puts("vulnerable");
exit(EXIT_SUCCESS);
}
if (retval == ERANGE) {
puts("not vulnerable");
exit(EXIT_SUCCESS);
}
```

## Important Update for Linux GHOST Vulnerability February 2015

```
}  
puts("should not happen");  
exit(EXIT_FAILURE);  
}
```

2. Compile `ghost.c` with the following command: `gcc ghost.c -o gh`  
**Notes:** You can compile this on another machine, and move to your HP Propel system(s). If needed, install the latest version of gcc, the GNU Compiler Collection, from <https://gcc.gnu.org/>.
3. Run the compiled file: `./gh` on the HP Propel Portal and the HP Propel Service eXchange (SX) system(s). Note that starting with Propel 1.10, there is a single Propel VM.
4. If the output is *not vulnerable*, your glibc is free of GHOST and no further action is needed. **If the output is *vulnerable***, you are using a vulnerable glibc and should complete the steps that follow.

### Action to remove vulnerability

To assure that the Linux GHOST Vulnerability will not affect your HP Propel system(s), complete the steps that follow.

5. Update glibc for CentOS on your HP Propel system(s) by running the following command:  

```
yum update glibc && reboot
```
6. Verify that the HP Propel services have restarted by running the following command:  

```
propel status
```
7. Confirm that GHOST vulnerability has been removed by repeating step 3 (run `./gh`). The output should now be *not vulnerable*.

For further information, go to: <https://access.redhat.com/articles/1332213>