



**AKATI  
CONSULTING  
PVT LTD**

**CVE-2015-0235 – HOW TO SECURE  
AGAINST GLIBC GHOST  
VULNERABILITY**

CVE-2015-0235



**Author | Rajivarnan.R Cyber security Researcher at Akati consulting  
Pvt Ltd**

## Description

Heap-based buffer overflow in the `__nss_hostname_digits_dots` function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) `gethostbyname` or (2) `gethostbyname2` function, aka "GHOST."

The GHOST vulnerability is a serious weakness in the Linux glibc library. It allows attackers to remotely take complete control of the victim system without having any prior knowledge of system credentials. CVE-2015-0235 has been assigned to this issue.

Qualys security researchers discovered this bug and worked closely with Linux distribution vendors. And as a result of that we are releasing this advisory today as a coordinated effort, and patches for all distribution are available January 27, 2015.

## What is glibc?

The GNU C Library or glibc is an implementation of the standard C library and a core part of the Linux operating system. Without this library a Linux system will not function.

## What is the vulnerability?

During a code audit Qualys researchers discovered a buffer overflow in the `__nss_hostname_digits_dots()` function of glibc. This bug can be triggered both locally and remotely via all the `gethostbyname*()` functions. Applications have access to the DNS resolver primarily through the `gethostbyname*()` set of functions. These functions convert a hostname into an IP address.

During a code audit performed internally at Qualys, discovered a buffer overflow in the `__nss_hostname_digits_dots()` function of the GNU C Library (glibc). This bug is reachable both locally and remotely via the `gethostbyname*()` functions, so we decided to analyze it -- and its impact -- thoroughly, and named this vulnerability "GHOST".

Main conclusions are:

- ❖ Via `gethostbyname()` or `gethostbyname2()`, the overflowed buffer is located in the heap. Via `gethostbyname_r()` or `gethostbyname2_r()`, the overflowed buffer is caller-supplied (and may therefore be located in the heap, stack, `.data`, `.bss`, etc; however, we have seen no such call in practice).
- ❖ At most size of `(char *)` bytes can be overwritten (ie, 4 bytes on 32-bit machines, and 8 bytes on 64-bit machines). Bytes can be overwritten only with digits ('0'...'9'), dots ('.'), and a terminating null character ('\0').

- ❖ Despite these limitations, arbitrary code execution can be achieved. As a proof of concept, we developed a full-fledged remote exploit against the Exim mail server, bypassing all existing protections (ASLR, PIE, and NX) on both 32-bit and 64-bit machines. We will publish our exploit as a Metasploit module in the near future.
- ❖ The first vulnerable version of the GNU C Library is glibc-2.2, released on November 10, 2000.
- ❖ We identified a number of factors that mitigate the impact of this bug. In particular, we discovered that it was fixed on May 21, 2013 (between the releases of glibc-2.17 and glibc-2.18). Unfortunately, it was not recognized as a security threat; as a result, most stable and long-term-support distributions were left exposed (and still are): Debian 7 (wheezy), Red Hat Enterprise Linux 6 & 7, CentOS 6 & 7, Ubuntu 12.04, for example.

## Analysis

The vulnerable function, `__nss_hostname_digits_dots()`, is called internally by the glibc in `nss/getXXbyYY.c` (the non-reentrant version) and `nss/getXXbyYY_r.c` (the reentrant version). However, the calls are surrounded by `#ifdef HANDLE_DIGITS_DOTS`, a macro defined only in:

- `inet/getstbynm.c`
- `inet/getstbynm2.c`
- `inet/getstbynm_r.c`
- `inet/getstbynm2_r.c`
- `nscd/getstbynm3_r.c`

These files implement the `gethostbyname*()` family, and hence the only way to reach `__nss_hostname_digits_dots()` and its buffer overflow. The purpose of this function is to avoid expensive DNS lookups if the hostname argument is already an IPv4 or IPv6 address.

The code below comes from glibc-2.17:

```
35 int
36 __nss_hostname_digits_dots (const char *name, struct hostent *resbuf,
37                             char **buffer, size_t *buffer_size,
38                             size_t buflen, struct hostent **result,
39                             enum nss_status *status, int af, int *h_errnop)
40 {
41     ..
42     ..
43     ..
44     ..
45     ..
46     ..
47     ..
48     ..
49     ..
50     ..
51     ..
52     ..
53     ..
54     ..
55     ..
56     ..
57     if (isdigit (name[0]) || isxdigit (name[0]) || name[0] == ':')
58     {
59         const char *cp;
60         char *hostname;
61         typedef unsigned char host_addr_t[16];
62         host_addr_t *host_addr;
63         typedef char *host_addr_list_t[2];
64         host_addr_list_t *h_addr_ptrs;
65         char **h_alias_ptr;
66         size_t size_needed;
67     }
68     ..
69     ..
70     ..
71     ..
72     ..
73     ..
74     ..
75     ..
76     ..
77     ..
78     ..
79     ..
80     ..
81     ..
82     ..
83     ..
84     ..
85     ..
86     ..
87     ..
88     ..
89     ..
90     ..
91     ..
92     ..
93     ..
94     ..
95     ..
96     ..
97     ..
98     ..
99     ..
100    ..
101    ..
102    ..
103    ..
104    ..
105    ..
106    ..
107    ..
108    ..
109    ..
110    ..
111    ..
112    ..
113    ..
114    ..
115    ..
116    ..
117    ..
118    ..
119    ..
120    ..
121    ..
122    ..
123    ..
124    ..
125    ..
126    ..
127    ..
128    ..
129    ..
130    ..
131    ..
132    ..
133    ..
134    ..
135    ..
136    ..
137    ..
138    ..
139    ..
140    ..
141    ..
142    ..
143    ..
144    ..
145    ..
146    ..
147    ..
148    ..
149    ..
150    ..
151    ..
152    ..
153    ..
154    ..
155    ..
156    ..
157    ..
158    ..
159    ..
160    ..
161    ..
162    ..
163    ..
164    ..
165    ..
166    ..
167    ..
168    ..
169    ..
170    ..
171    ..
172    ..
173    ..
174    ..
175    ..
176    ..
177    ..
178    ..
179    ..
180    ..
181    ..
182    ..
183    ..
184    ..
185    ..
186    ..
187    ..
188    ..
189    ..
190    ..
191    ..
192    ..
193    ..
194    ..
195    ..
196    ..
197    ..
198    ..
199    ..
200    ..
201    ..
202    ..
203    ..
204    ..
205    ..
206    ..
207    ..
208    ..
209    ..
210    ..
211    ..
212    ..
213    ..
214    ..
215    ..
216    ..
217    ..
218    ..
219    ..
220    ..
221    ..
222    ..
223    ..
224    ..
225    ..
226    ..
227    ..
228    ..
229    ..
230    ..
231    ..
232    ..
233    ..
234    ..
235    ..
236    ..
237    ..
238    ..
239    ..
240    ..
241    ..
242    ..
243    ..
244    ..
245    ..
246    ..
247    ..
248    ..
249    ..
250    ..
251    ..
252    ..
253    ..
254    ..
255    ..
256    ..
257    ..
258    ..
259    ..
260    ..
261    ..
262    ..
263    ..
264    ..
265    ..
266    ..
267    ..
268    ..
269    ..
270    ..
271    ..
272    ..
273    ..
274    ..
275    ..
276    ..
277    ..
278    ..
279    ..
280    ..
281    ..
282    ..
283    ..
284    ..
285    ..
286    ..
287    ..
288    ..
289    ..
290    ..
291    ..
292    ..
293    ..
294    ..
295    ..
296    ..
297    ..
298    ..
299    ..
300    ..
301    ..
302    ..
303    ..
304    ..
305    ..
306    ..
307    ..
308    ..
309    ..
310    ..
311    ..
312    ..
313    ..
314    ..
315    ..
316    ..
317    ..
318    ..
319    ..
320    ..
321    ..
322    ..
323    ..
324    ..
325    ..
326    ..
327    ..
328    ..
329    ..
330    ..
331    ..
332    ..
333    ..
334    ..
335    ..
336    ..
337    ..
338    ..
339    ..
340    ..
341    ..
342    ..
343    ..
344    ..
345    ..
346    ..
347    ..
348    ..
349    ..
350    ..
351    ..
352    ..
353    ..
354    ..
355    ..
356    ..
357    ..
358    ..
359    ..
360    ..
361    ..
362    ..
363    ..
364    ..
365    ..
366    ..
367    ..
368    ..
369    ..
370    ..
371    ..
372    ..
373    ..
374    ..
375    ..
376    ..
377    ..
378    ..
379    ..
380    ..
381    ..
382    ..
383    ..
384    ..
385    ..
386    ..
387    ..
388    ..
389    ..
390    ..
391    ..
392    ..
393    ..
394    ..
395    ..
396    ..
397    ..
398    ..
399    ..
400    ..
401    ..
402    ..
403    ..
404    ..
405    ..
406    ..
407    ..
408    ..
409    ..
410    ..
411    ..
412    ..
413    ..
414    ..
415    ..
416    ..
417    ..
418    ..
419    ..
420    ..
421    ..
422    ..
423    ..
424    ..
425    ..
426    ..
427    ..
428    ..
429    ..
430    ..
431    ..
432    ..
433    ..
434    ..
435    ..
436    ..
437    ..
438    ..
439    ..
440    ..
441    ..
442    ..
443    ..
444    ..
445    ..
446    ..
447    ..
448    ..
449    ..
450    ..
451    ..
452    ..
453    ..
454    ..
455    ..
456    ..
457    ..
458    ..
459    ..
460    ..
461    ..
462    ..
463    ..
464    ..
465    ..
466    ..
467    ..
468    ..
469    ..
470    ..
471    ..
472    ..
473    ..
474    ..
475    ..
476    ..
477    ..
478    ..
479    ..
480    ..
481    ..
482    ..
483    ..
484    ..
485    ..
486    ..
487    ..
488    ..
489    ..
490    ..
491    ..
492    ..
493    ..
494    ..
495    ..
496    ..
497    ..
498    ..
499    ..
500    ..
501    ..
502    ..
503    ..
504    ..
505    ..
506    ..
507    ..
508    ..
509    ..
510    ..
511    ..
512    ..
513    ..
514    ..
515    ..
516    ..
517    ..
518    ..
519    ..
520    ..
521    ..
522    ..
523    ..
524    ..
525    ..
526    ..
527    ..
528    ..
529    ..
530    ..
531    ..
532    ..
533    ..
534    ..
535    ..
536    ..
537    ..
538    ..
539    ..
540    ..
541    ..
542    ..
543    ..
544    ..
545    ..
546    ..
547    ..
548    ..
549    ..
550    ..
551    ..
552    ..
553    ..
554    ..
555    ..
556    ..
557    ..
558    ..
559    ..
560    ..
561    ..
562    ..
563    ..
564    ..
565    ..
566    ..
567    ..
568    ..
569    ..
570    ..
571    ..
572    ..
573    ..
574    ..
575    ..
576    ..
577    ..
578    ..
579    ..
580    ..
581    ..
582    ..
583    ..
584    ..
585    ..
586    ..
587    ..
588    ..
589    ..
590    ..
591    ..
592    ..
593    ..
594    ..
595    ..
596    ..
597    ..
598    ..
599    ..
600    ..
601    ..
602    ..
603    ..
604    ..
605    ..
606    ..
607    ..
608    ..
609    ..
610    ..
611    ..
612    ..
613    ..
614    ..
615    ..
616    ..
617    ..
618    ..
619    ..
620    ..
621    ..
622    ..
623    ..
624    ..
625    ..
626    ..
627    ..
628    ..
629    ..
630    ..
631    ..
632    ..
633    ..
634    ..
635    ..
636    ..
637    ..
638    ..
639    ..
640    ..
641    ..
642    ..
643    ..
644    ..
645    ..
646    ..
647    ..
648    ..
649    ..
650    ..
651    ..
652    ..
653    ..
654    ..
655    ..
656    ..
657    ..
658    ..
659    ..
660    ..
661    ..
662    ..
663    ..
664    ..
665    ..
666    ..
667    ..
668    ..
669    ..
670    ..
671    ..
672    ..
673    ..
674    ..
675    ..
676    ..
677    ..
678    ..
679    ..
680    ..
681    ..
682    ..
683    ..
684    ..
685    ..
686    ..
687    ..
688    ..
689    ..
690    ..
691    ..
692    ..
693    ..
694    ..
695    ..
696    ..
697    ..
698    ..
699    ..
700    ..
701    ..
702    ..
703    ..
704    ..
705    ..
706    ..
707    ..
708    ..
709    ..
710    ..
711    ..
712    ..
713    ..
714    ..
715    ..
716    ..
717    ..
718    ..
719    ..
720    ..
721    ..
722    ..
723    ..
724    ..
725    ..
726    ..
727    ..
728    ..
729    ..
730    ..
731    ..
732    ..
733    ..
734    ..
735    ..
736    ..
737    ..
738    ..
739    ..
740    ..
741    ..
742    ..
743    ..
744    ..
745    ..
746    ..
747    ..
748    ..
749    ..
750    ..
751    ..
752    ..
753    ..
754    ..
755    ..
756    ..
757    ..
758    ..
759    ..
760    ..
761    ..
762    ..
763    ..
764    ..
765    ..
766    ..
767    ..
768    ..
769    ..
770    ..
771    ..
772    ..
773    ..
774    ..
775    ..
776    ..
777    ..
778    ..
779    ..
780    ..
781    ..
782    ..
783    ..
784    ..
785    ..
786    ..
787    ..
788    ..
789    ..
790    ..
791    ..
792    ..
793    ..
794    ..
795    ..
796    ..
797    ..
798    ..
799    ..
800    ..
801    ..
802    ..
803    ..
804    ..
805    ..
806    ..
807    ..
808    ..
809    ..
810    ..
811    ..
812    ..
813    ..
814    ..
815    ..
816    ..
817    ..
818    ..
819    ..
820    ..
821    ..
822    ..
823    ..
824    ..
825    ..
826    ..
827    ..
828    ..
829    ..
830    ..
831    ..
832    ..
833    ..
834    ..
835    ..
836    ..
837    ..
838    ..
839    ..
840    ..
841    ..
842    ..
843    ..
844    ..
845    ..
846    ..
847    ..
848    ..
849    ..
850    ..
851    ..
852    ..
853    ..
854    ..
855    ..
856    ..
857    ..
858    ..
859    ..
860    ..
861    ..
862    ..
863    ..
864    ..
865    ..
866    ..
867    ..
868    ..
869    ..
870    ..
871    ..
872    ..
873    ..
874    ..
875    ..
876    ..
877    ..
878    ..
879    ..
880    ..
881    ..
882    ..
883    ..
884    ..
885    ..
886    ..
887    ..
888    ..
889    ..
890    ..
891    ..
892    ..
893    ..
894    ..
895    ..
896    ..
897    ..
898    ..
899    ..
900    ..
901    ..
902    ..
903    ..
904    ..
905    ..
906    ..
907    ..
908    ..
909    ..
910    ..
911    ..
912    ..
913    ..
914    ..
915    ..
916    ..
917    ..
918    ..
919    ..
920    ..
921    ..
922    ..
923    ..
924    ..
925    ..
926    ..
927    ..
928    ..
929    ..
930    ..
931    ..
932    ..
933    ..
934    ..
935    ..
936    ..
937    ..
938    ..
939    ..
940    ..
941    ..
942    ..
943    ..
944    ..
945    ..
946    ..
947    ..
948    ..
949    ..
950    ..
951    ..
952    ..
953    ..
954    ..
955    ..
956    ..
957    ..
958    ..
959    ..
960    ..
961    ..
962    ..
963    ..
964    ..
965    ..
966    ..
967    ..
968    ..
969    ..
970    ..
971    ..
972    ..
973    ..
974    ..
975    ..
976    ..
977    ..
978    ..
979    ..
980    ..
981    ..
982    ..
983    ..
984    ..
985    ..
986    ..
987    ..
988    ..
989    ..
990    ..
991    ..
992    ..
993    ..
994    ..
995    ..
996    ..
997    ..
998    ..
999    ..
1000   ..
1001   ..
1002   ..
1003   ..
1004   ..
1005   ..
1006   ..
1007   ..
1008   ..
1009   ..
1010   ..
1011   ..
1012   ..
1013   ..
1014   ..
1015   ..
1016   ..
1017   ..
1018   ..
1019   ..
1020   ..
1021   ..
1022   ..
1023   ..
1024   ..
1025   ..
1026   ..
1027   ..
1028   ..
1029   ..
1030   ..
1031   ..
1032   ..
1033   ..
1034   ..
1035   ..
1036   ..
1037   ..
1038   ..
1039   ..
1040   ..
1041   ..
1042   ..
1043   ..
1044   ..
1045   ..
1046   ..
1047   ..
1048   ..
1049   ..
1050   ..
1051   ..
1052   ..
1053   ..
1054   ..
1055   ..
1056   ..
1057   ..
1058   ..
1059   ..
1060   ..
1061   ..
1062   ..
1063   ..
1064   ..
1065   ..
1066   ..
1067   ..
1068   ..
1069   ..
1070   ..
1071   ..
1072   ..
1073   ..
1074   ..
1075   ..
1076   ..
1077   ..
1078   ..
1079   ..
1080   ..
1081   ..
1082   ..
1083   ..
1084   ..
1085   ..
1086   ..
1087   ..
1088   ..
1089   ..
1090   ..
1091   ..
1092   ..
1093   ..
1094   ..
1095   ..
1096   ..
1097   ..
1098   ..
1099   ..
1100   ..
1101   ..
1102   ..
1103   ..
1104   ..
1105   ..
1106   ..
1107   ..
1108   ..
1109   ..
1110   ..
1111   ..
1112   ..
1113   ..
1114   ..
1115   ..
1116   ..
1117   ..
1118   ..
1119   ..
1120   ..
1121   ..
1122   ..
1123   ..
1124   ..
1125   ..
1126   ..
1127   ..
1128   ..
1129   ..
1130   ..
1131   ..
1132   ..
1133   ..
1134   ..
1135   ..
1136   ..
1137   ..
1138   ..
1139   ..
1140   ..
1141   ..
1142   ..
1143   ..
1144   ..
1145   ..
1146   ..
1147   ..
1148   ..
1149   ..
1150   ..
1151   ..
1152   ..
1153   ..
1154   ..
1155   ..
1156   ..
1157   ..
1158   ..
1159   ..
1160   ..
1161   ..
1162   ..
1163   ..
1164   ..
1165   ..
1166   ..
1167   ..
1168   ..
1169   ..
1170   ..
1171   ..
1172   ..
1173   ..
1174   ..
1175   ..
1176   ..
1177   ..
1178   ..
1179   ..
1180   ..
1181   ..
1182   ..
1183   ..
1184   ..
1185   ..
1186   ..
1187   ..
1188   ..
1189   ..
1190   ..
1191   ..
1192   ..
1193   ..
1194   ..
1195   ..
1196   ..
1197   ..
1198   ..
1199   ..
1200   ..
1201   ..
1202   ..
1203   ..
1204   ..
1205   ..
1206   ..
1207   ..
1208   ..
1209   ..
1210   ..
1211   ..
1212   ..
1213   ..
1214   ..
1215   ..
1216   ..
1217   ..
1218   ..
1219   ..
1220   ..
1221   ..
1222   ..
1223   ..
1224   ..
1225   ..
1226   ..
1227   ..
1228   ..
1229   ..
1230   ..
1231   ..
1232   ..
1233   ..
1234   ..
1235   ..
1236   ..
1237   ..
1238   ..
1239   ..
1240   ..
1241   ..
1242   ..
1243   ..
1244   ..
1245   ..
1246   ..
1247   ..
1248   ..
1249   ..
1250   ..
1251   ..
1252   ..
1253   ..
1254   ..
1255   ..
1256   ..
1257   ..
1258   ..
1259   ..
1260   ..
1261   ..
1262   ..
1263   ..
1264   ..
1265   ..
1266   ..
1267   ..
1268   ..
1269   ..
1270   ..
1271   ..
1272   ..
1273   ..
1274   ..
1275   ..
1276   ..
1277   ..
1278   ..
1279   ..
1280   ..
1281   ..
1282   ..
1283   ..
1284   ..
1285   ..
1286   ..
1287   ..
1288   ..
1289   ..
1290   ..
1291   ..
1292   ..
1293   ..
1294   ..
1295   ..
1296   ..
1297   ..
1298   ..
1299   ..
1300   ..
1301   ..
1302   ..
1303   ..
1304   ..
1305   ..
1306   ..
1307   ..
1308   ..
1309   ..
1310   ..
1311   ..
1312   ..
1313   ..
1314   ..
1315   ..
1316   ..
1317   ..
1318   ..
1319   ..
1320   ..
1321   ..
1322   ..
1323   ..
1324   ..
1325   ..
1326   ..
1327   ..
1328   ..
1329   ..
1330   ..
1331   ..
1332   ..
1333   ..
1334   ..
1335   ..
1336   ..
1337   ..
1338   ..
1339   ..
1340   ..
1341   ..
1342   ..
1343   ..
1344   ..
1345   ..
1346   ..
1347   ..
1348   ..
1349   ..
1350   ..
1351   ..
1352   ..
1353   ..
1354   ..
1355   ..
1356   ..
1357   ..
1358   ..
1359   ..
1360   ..
1361   ..
1362   ..
1363   ..
1364   ..
1365   ..
1366   ..
1367   ..
1368   ..
1369   ..
1370   ..
1371   ..
1372   ..
1373   ..
1374   ..
1375   ..
1376   ..
1377   ..
1378   ..
1379   ..
1380   ..
1381   ..
1382   ..
1383   ..
1384   ..
1385   ..
1386   ..
1387   ..
1388   ..
1389   ..
1390   ..
1391   ..
1392   ..
1393   ..
1394   ..
1395   ..
1396   ..
1397   ..
1398   ..
1399   ..
1400   ..
1401   ..
1402   ..
1403   ..
1404   ..
1405   ..
1406   ..
1407   ..
1408   ..
1409   ..
1410   ..
1411   ..
1412   ..
1413   ..
1414   ..
1415   ..
1416   ..
1417   ..
1418   ..
1419   ..
1420   ..
1421   ..
1422   ..
1423   ..
1424   ..
1425   ..
1426   ..
1427   ..
1428   ..
1429   ..
1430   ..
1431   ..
1432   ..
1433   ..
1434   ..
1435   ..
1436   ..
1437   ..
1438   ..
1439   ..
1440   ..
1441   ..
1442   ..
1443   ..
1444   ..
1445   ..
1446   ..
1447   ..
1448   ..
1449   ..
1450   ..
1451   ..
1452   ..
1453   ..
1454   ..
1455   ..
1456   ..
1457   ..
1458   ..
1459   ..
1460   ..
1461   ..
1462   ..
1463   ..
1464   ..
1465   ..
1466   ..
1467   ..
1468   ..
1469   ..
1470   ..
1471   ..
1472   ..
1473   ..
1474   ..
1475   ..
1476   ..
1477   ..
1478   ..
1479   ..
1480   ..
1481   ..
1482   ..
1483   ..
1484   ..
1485   ..
1486   ..
1487   ..
1488   ..
1489   ..
1490   ..
1491   ..
1492   ..
1493   ..
1494   ..
1495   ..
1496   ..
1497   ..
1498   ..
1499   ..
1500   ..
1501   ..
1502   ..
1503   ..
1504   ..
1505   ..
1506   ..
1507   ..
1508   ..
1509   ..
1510   ..
1511   ..
1512   ..
1513   ..
1514   ..
1515   ..
1516   ..
1517   ..
1518   ..
1519   ..
1520   ..
1521   ..
1522   ..
1523   ..
1524   ..
1525   ..
1526   ..
1527   ..
1528   ..
1529   ..
1530   ..
1531   ..
1532   ..
1533   ..
1534   ..
1535   ..
1536   ..
1537   ..
1538   ..
1539   ..
1540   ..
1541   ..
1542   ..
1543   ..
1544   ..
1545   ..
1546   ..
1547   ..
1548   ..
1549   ..
1550   ..
1551   ..
1552   ..
1553   ..
1554   ..
1555   ..
1556   ..
1557   ..
1558   ..
1559   ..
1560   ..
1561   ..
1562   ..
1563   ..
1564   ..
1565   ..
1566   ..
1567   ..
1568   ..
1569   ..
1570   ..
1571   ..
1572   ..
1573   ..
1574   ..
1575   ..
1576   ..
1577   ..
1578   ..
1579   ..
1580   ..
1581   ..
1582   ..
1583   ..
1584   ..
1585   ..
1586   ..
1587   ..
1588   ..
1589   ..
1590   ..
1591   ..
1592   ..
1593   ..
1594   ..
1595   ..
1596   ..
1597   ..
1598   ..
1599   ..
1600   ..
1601   ..
1602   ..
1603   ..
1604   ..
1605   ..
1606   ..
1607   ..
1608   ..
1609   ..
1610   ..
1611   ..
1612   ..
1613   ..
1614   ..
1615   ..
1616   ..
1617   ..
1618   ..
1619   ..
1620   ..
1621   ..
1622   ..
1623   ..
1624   ..
1625   ..
1626   ..
1627   ..
1628   ..
1629   ..
1630   ..
1631   ..
1632   ..
1633   ..
1634   ..
1635   ..
1636   ..
1637   ..
1638   ..
1639   ..
1640   ..
1641   ..
1642   ..
1643   ..
1644   ..
1645   ..
1646   ..
1647   ..
1648   ..
1649   ..
1650   ..
1651   ..
1652   ..
1653   ..
1654   ..
1655   ..
1656   ..
1657   ..
1658   ..
1659   ..
1660   ..
1661   ..
1662   ..
1663   ..
1664   ..
1665   ..
1666   ..
1667   ..
1668   ..
1669   ..
1670   ..
1671   ..
1672   ..
1673   ..
1674   ..
1675   ..
1676   ..
1677   ..
1678   ..
1679   ..
1680   ..
1681   ..
1682   ..
1683   ..
1684   ..
1685   ..
1686   ..
1687   ..
1688   ..
1689   ..
1690   ..
1691   ..
1692   ..
1693   ..
1694   ..
1695   ..
1696   ..
1697   ..
1698   ..
1699   ..
1700   ..
1701   ..
1702   ..
1703   ..
1704   ..
1705   ..
1706   ..
1707   ..
1708   ..
1709   ..
1710   ..
1711   ..
1712   ..
1713   ..
1714   ..
1715   ..
1716   ..
1717   ..
1718   ..
1719   ..
1720   ..
1721   ..
1722   ..
1723   ..
1724   ..
1725   ..
1726   ..
1727   ..
1728   ..
1729   ..
1730   ..
1731   ..
1732   ..
1733   ..
1734   ..
1735   ..
1736   ..
1737   ..
1738   ..
1739   ..
1740   ..
1741   ..
1742   ..
1743   ..
1744   ..
1745   ..
1746   ..
1747   ..
1748   ..
1749   ..
1750   ..
1751   ..
1752   ..
1753   ..
1754   ..
1755   ..
1756   ..
1757   ..
1758   ..
1759   ..
1760   ..
1761   ..
1762   ..
1763   ..
1764   ..
1765   ..
1766   ..
1767   ..
1768   ..
1769   ..
1770   ..
1771   ..
1772   ..
1773   ..
1774   ..
1775   ..
1776   ..
1777   ..
1778   ..
1779   ..
1780   ..
1781   ..
1782   ..
1783   ..
1784   ..
1785   ..
1786   ..
1787   ..
1788   ..
1789   ..
1790   ..
1791   ..
1792   ..
1793   ..
1794   ..
1795   ..
1796   ..
1797   ..
1798   ..
1799   ..
1800   ..
1801   ..
1802   ..
1803   ..
1804   ..
1805   ..
1806   ..
1807   ..
1808   ..
1809   ..
1810   ..
1811   ..
1812   ..
1813   ..
1814   ..
1815   ..
1816   ..
1817   ..
1818   ..
1819   ..
1820   ..
1821   ..
1822   ..
1823  
```

```
85     size_needed = (sizeof (*host_addr)
86                   + sizeof (*h_addr_ptrs) + strlen (name) + 1);
87
88     if (buffer_size == NULL)
89     {
90         if (buflen < size_needed)
91         {
92             ..
93             goto done;
94         }
95     }
96     else if (buffer_size != NULL && *buffer_size < size_needed)
97     {
98         char *new_buf;
99         *buffer_size = size_needed;
100        new_buf = (char *) realloc (*buffer, *buffer_size);
101
102        if (new_buf == NULL)
103        {
104            ..
105            goto done;
106        }
107        *buffer = new_buf;
108    }
109
110    ..
111    host_addr = (host_addr_t *) *buffer;
112    h_addr_ptrs = (host_addr_list_t *)
113        ((char *) host_addr + sizeof (*host_addr));
114    h_alias_ptr = (char **) ((char *) h_addr_ptrs + sizeof (*h_addr_ptrs));
115    hostname = (char *) h_alias_ptr + sizeof (*h_alias_ptr);
116
117    if (isdigit (name[0]))
118    {
119        for (cp = name;; ++cp)
120        {
121            if (*cp == '\0')
122            {
123                int ok;
124
125                if (*--cp == '.')
126                    break;
127
128                ..
129                if (af == AF_INET)
130                    ok = __inet_aton (name, (struct in_addr *) host_addr);
131                else
132                {
133                    assert (af == AF_INET6);
134                    ok = inet_pton (af, name, host_addr) > 0;
135                }
136                if (! ok)
137                {
```

```

...
154         goto done;
155     }
156
157     resbuf->h_name = strcpy (hostname, name);
...
194     goto done;
195 }
196
197     if (!isdigit (*cp) && *cp != '.')
198         break;
199 }
200 }
...

```

Lines 85-86 compute the `size_needed` to store three (3) distinct entities in buffer: `host_addr`, `h_addr_ptrs`, and `name` (the hostname). Lines 88-117 make sure the buffer is large enough: lines 88-97 correspond to the reentrant case, lines 98-117 to the non-reentrant case.

Lines 121-125 prepare pointers to store four (4) distinct entities in buffer: `host_addr`, `h_addr_ptrs`, `h_alias_ptr`, and `hostname`. The `sizeof (*h_alias_ptr)` -- the size of a char pointer -- is missing from the computation of `size_needed`.

The `strcpy()` on line 157 should therefore allow us to write past the end of buffer, at most (depending on `strlen(name)` and alignment) 4 bytes on 32-bit machines, or 8 bytes on 64-bit machines. There is a similar `strcpy()` after line 200, but no buffer overflow:

```

236     size_needed = (sizeof (*host_addr)
237                 + sizeof (*h_addr_ptrs) + strlen (name) + 1);
...
267     host_addr = (host_addr_t *) *buffer;
268     h_addr_ptrs = (host_addr_list_t *)
269         ((char *) host_addr + sizeof (*host_addr));
270     hostname = (char *) h_addr_ptrs + sizeof (*h_addr_ptrs);
...
289     resbuf->h_name = strcpy (hostname, name);

```

In order to reach the overflow at line 157, the `hostname` argument must meet the following requirements:

- ❖ Its first character must be a digit (line 127).
- ❖ Its last character must not be a dot (line 135).
- ❖ It must comprise only digits and dots (line 197) (we call this the "digits-and-dots" requirement).
- ❖ It must be long enough to overflow the buffer. For example, the non-reentrant `gethostbyname*`() functions initially allocate their buffer with a call to `malloc(1024)` (the "1-KB" requirement).

- ❖ It must be successfully parsed as an IPv4 address by `inet_aton()` (line 143), or as an IPv6 address by `inet_pton()` (line 147). Upon careful analysis of these two functions, we can further refine this "inet-aton" requirement:
- ❖ It is impossible to successfully parse a "digits-and-dots" hostname as an IPv6 address with `inet_pton()` (':' is forbidden). Hence it is impossible to reach the overflow with calls to `gethostbyname2()` or `gethostbyname2_r()` if the address family argument is `AF_INET6`.
- ❖ . Conclusion: `inet_aton()` is the only option, and the hostname must have one of the following forms: "a.b.c.d", "a.b.c", "a.b", or "a", where a, b, c, d must be unsigned integers, at most 0xffffffff, converted successfully (ie, no integer overflow) by `strtoul()` in decimal or octal (but not hexadecimal, because 'x' and 'X' are forbidden).

## Impact of this Bug

The impact of this bug is reduced significantly by the following Reasons:

- ❖ A patch already exists (since May 21, 2013), and has been applied and tested since glibc-2.18, released on August 12, 2013:

[BZ #15014]

- `nss/getXXbyYY_r.c (INTERNAL (REENTRANT_NAME))`

[HANDLE\_DIGITS\_DOTS]: Set `any_service` when digits-dots parsing was successful.

- `nss/digits_dots.c (__nss_hostname_digits_dots)`: Remove redundant variable declarations and reallocation of buffer when parsing as IPv6 address. Always set NSS status when called from reentrant functions. Use `NETDB_INTERNAL` instead of `TRY_AGAIN` when buffer too small. Correct computation of needed size.
- `nss/Makefile (tests)`: Add test-digits-dots.
- `nss/test-digits-dots.c`: New test.

- ❖ The `gethostbyname*()` functions are obsolete; with the advent of IPv6, recent applications use `getaddrinfo()` instead.
- ❖ Many programs, especially SUID binaries reachable locally, use `gethostbyname()` if, and only if, a preliminary call to `inet_aton()` fails. However, a subsequent call must also succeed (the "inet-aton" requirement) in order to reach the overflow: this is impossible, and such programs are therefore safe.
- ❖ Most of the other programs, especially servers reachable remotely, use `gethostbyname()` to perform forward-confirmed reverse DNS (FCrDNS, also known as full-circle reverse DNS) checks. These programs are generally safe, because the hostname passed to `gethostbyname()` has normally been pre-validated by DNS software:

"a string of labels each containing up to 63 8-bit octets, separated by dots, and with a maximum total of 255 octets." This makes it impossible to satisfy the "1-KB" requirement.

Actually, glibc's DNS resolver can produce hostnames of up to (almost) 1025 characters (in case of bit-string labels, and special or non-printable characters). But this introduces backslashes ("\") and makes it impossible to satisfy the "digits-and-dots" requirement.

## Case Study

In this section, we will analyze real-world examples of programs that call the `gethostbyname*` functions, but we first introduce a small test program that checks whether a system is vulnerable or not:

```
[user () fedora-19 ~]$ cat > GHOST.c << EOF
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.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);
    }
    puts("should not happen");
    exit(EXIT_FAILURE);
}
EOF
```

```
[user () fedora-19 ~]$ gcc GHOST.c -o GHOST
```

On Fedora 19 (glibc-2.17):

```
[user () fedora-19 ~]$ ./GHOST  
vulnerable
```

On Fedora 20 (glibc-2.18):

```
[user () fedora-20 ~]$ ./GHOST  
not vulnerable
```

## What versions and operating systems are affected?

The first vulnerable version of the GNU C Library affected by this is glibc-2.2, released on November 10, 2000. We identified a number of factors that mitigate the impact of this bug. In particular, we discovered that it was fixed on May 21, 2013 (between the releases of glibc-2.17 and glibc-2.18). Unfortunately, it was not recognized as a security threat; as a result, most stable and long-term-support distributions were left exposed including Debian 7 (wheezy), Red Hat Enterprise Linux 6 & 7, CentOS 6 & 7, Ubuntu 12.04, for example.

## Following are the potentially exploitable services

- Procmal
- Exim
- Pppd
- Clockdiff

You can find the list of services which are rely on the GNU C libraries by executing following command

**Code:**  
**lsuf | grep libc | awk '{print \$1}' | sort | uni**

## Fix for Centos/RHEL/Fedora 5,6,7

### Code:

```
yum update glibc  
sudo restart
```

## Fix for Ubuntu

### Code:

```
sudo apt-get update  
sudo apt-get dist-upgrade  
sudo restart
```

Thank you