Silver Peak Security Advisory

CVE-2015-7547, published by NIST on 02/18/2016

glibc getaddrinfo stack-based buffer overflow

Summary:

US-CERT/NIST advisory for CVE-2015-7547 is dated 02/18/2016.

The advisory is about multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.

GNU C Library (glibc) versions 2.9 through 2.22 are affected by this stack-based buffer overflow vulnerability.

glibc versions used on Orchestrator:
Orchestrator on fc12 has glibc version 2.11
Orchestrator on fc14 has glibc version 2.13

glibc version on VXOA appliances:
glibc version 2.5

Silver Peak Orchestrator (GMS) is vulnerable to this vulnerability.

Silver Peak VXOA appliances are not susceptible to this vulnerability.

Patch to resolve the vulnerability is detailed under 'Resolution' heading below.

Details:

CVE provides information on the advisory and is located at:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547

The full advisory located at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547

Details on this vulnerability is also at https://sourceware.org/bugzilla/show_bug.cgi?id=18665 **and reads as following:**

When the thisanssizp pointer variable on line 1257 is updated,
thisanssizp = anssizp2, i.e assigned a new address,
this change causes the thisanssizp pointer variable used in the
recvfrom function on line 1282 to use the
wrong size if a new buffer is created after the thisanssizp
address has been changed at line 1257.

The size of the buffer used will be what was stored at the
address assigned at line 1257, and not the size of the newly
created buffer.

The program will crash if the calculated size of the buffer used
is 0. The recvfrom function will
not crash, but any further accesses to the buffer where the
bytes read was 0 from the recvfrom function
will crash the program.

Initially at line 1230:
thisanssizp = anssizp;
-the thisanssizp gets assigned the address of anssizp when the
send_dg function is first called.

At line 1257:
thisanssizp = anssizp2;
-the thisanssizp address gets updated after we have received a
packet.

At line 1273:
*anssizp = MAXPACKET;
-the size of a new packet is assigned to *anssizp, and not
*thisanssizp, when a new buffer is created.

At line 1282:
recvfrom(pfd[0].fd, (char*)*thisansp, *thisanssizp,
-the recvfrom function uses the size from *thisanssizp which is
wrong.
-it can be seen here that thisansp will contain the address of a
newly created buffer, but the *thisanssizp, will contain the
size from the aligned_resplen, instead of MAXPACKET.

Fix:

```
Use the size pointer *thisanssizp, instead of *thisansp, when
creating the new buffer.

u_char *newp = malloc (MAXPACKET);
                    if (newp != NULL) {
                          <*anssizp = MAXPACKET;>      :REMOVED
LINE:
                          *thisanssizp = MAXPACKET;    :ADDED
LINE:
                          *thisansp = ans = newp;
                          if (thisansp == ansp2)
                            *ansp2_malloced = 1;
```

NIST has added the vulnerability summary for this CVE to their National Cyber Awareness System database:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7547

Recommended Action for Silver Peak Customers:

Silver Peak GMS (Orchestrator) product:
Silver Peak Orchestrator (GMS) is affected by this vulnerability. It is recommended to upgrade Orchestrator (GMS) to below mentioned releases to mitigate risk against the vulnerability. The patch is in line with the recommendation in the CVE-2015-7547 advisory.

Silver Peak VXOA appliances:
Silver Peak VXOA appliances are not affected by this vulnerability

Resolution:

Silver Peak Issue Id 30061 tracks this vulnerability.

The Resolution for this vulnerability is in each of the below mentioned branches of release:

Orchestrator (GMS) release 7.3.7 and later

Orchestrator (GMS) release 8.0.2 and later