[SA80907] SUSE update for kernel

Secunia Advisory ID	SA80907
Title	SUSE update for kernel
Release date	2018-01-05
Last update	2018-01-18
Criticality	- Less critical
Impact	Security Bypass, Exposure of sensitive information, Privilege escalation, DoS, System access
Where	From local network
Solution Status	Vendor Patched
Secunia CVSS Scores	Base: 7.2 , Overall: 5.3 (AV:L/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)
CVE references	CVE-2017-16538 | CVE-2017-11600 | CVE-2017-14106 | CVE-2017-13167 | CVE-2017-17450 | CVE-2017-17806 | CVE-2017-17558 | CVE-2017-5715 | CVE-2017-17805 | CVE-2017-7472 | CVE-2017-5754 | CVE-2017-16534 | CVE-2017-8824 | CVE-2017-15868 | CVE-2017-16939 | CVE-2017-5753 | CVE-2017-15115 |

Affected operating system and software

Operating systems

SUSE Linux Enterprise Server (SLES) 11

SUSE Linux Enterprise Server (SLES) 11 SP4

Advisory Details:

Description:

SUSE has issued an update for kernel. This fixes multiple vulnerabilities, which can be exploited by malicious people with physical access to compromise a vulnerable system, by malicious, local users to disclose potentially sensitive information, bypass certain security restrictions, cause a DoS (Denial of Service), and gain escalated privileges, and by malicious people to bypass certain security restrictions.

For more information:
SA76341 (#1)
SA77700 (#6)
SA78713 (#1)
SA78818 (#1)
SA80212 (#1)
SA80289 (#1)
SA80385 (#31)
SA80543 (#1)
SA80617 (#1)
SA80680 (#1)
SA80732 (#1)
SA80843 (#1 through #3)

1) An error related to sound timer can be exploited to gain elevated privileges.

Note: The vulnerabilities affect the EXTRA and SP4 versions only concerning the SUSE Linux Enterprise Server (SLES) 11 product.

Solution:

Apply updated packages via the zypper package manager.

Note: New packages have been released for "SUSE Linux Enterprise Server (SLES) 11 EXTRA" and "SUSE Linux Enterprise Server (SLES) 11 SP4" running on the IBM Z platform.

Provided and/or discovered by:

1) The vendor Android credits Qidan He (@flanker_hqd), KeenLab, Tencent.

Original advisory:

SUSE-SU-2018:0131-1:
https://www.suse.com/support/update/announcement/2018/suse-su-20180131-1/
Android:
https://source.android.com/security/bulletin/pixel/2017-12-01
SUSE-SU-2018:0011-1:
https://www.suse.com/support/update/announcement/2018/suse-su-20180011-1/

References:

SA80843:
SA80843
SA80617:
SA80617
SA80289:
SA80289
SA80543:
SA80543
SA76341:
SA76341
SA78713:
SA78713
SA80385:
SA80385
SA80732:
SA80732
SA80680:
SA80680
SA80212:
SA80212
SA78818:
SA78818
SA77700:
SA77700

Changelog:

2018-01-18: Updated the advisory due to an incomplete fix for CVE-2017-5753 and a regression caused in a previous update for "SUSE Linux Enterprise Server (SLES) 11 EXTRA" and "SUSE Linux Enterprise Server (SLES) 11 SP4". Added a link to the "Original Advisory" section. Updated the "Solution" section.
2018-01-05: Initial release