[SA80856] SUSE update for kernel

Secunia Advisory ID	SA80856
Title	SUSE update for kernel
Release date	2018-01-04
Last update	2018-01-11
Criticality	- Not critical
Impact	Exposure of sensitive information, Security Bypass, DoS
Where	Local system
Solution Status	Vendor Patched
Secunia CVSS Scores	Base: 4.6 , Overall: 3.4 (AV:L/AC:L/Au:S/C:N/I:N/A:C/E:U/RL:OF/RC:C)
CVE references	CVE-2017-5754 | CVE-2017-17805 | CVE-2017-5715 | CVE-2017-17806 | CVE-2017-5753 |

Affected operating system and software

Operating systems

SUSE Linux Enterprise Server (SLES) 12 SP2

Advisory Details:

Description:

SUSE has issued an update for kernel. This fixes multiple vulnerabilities, which can be exploited by malicious, local users to disclose sensitive information, bypass certain security restrictions, and cause a DoS (Denial of Service).

For more information:
SA80680 (#1)
SA80732 (#1)
SA80843 (#1 through #3)

Solution:

Apply updated packages via the zypper package manager.

Note: New packages have been released for "SUSE Linux Enterprise Server (SLES) 12 SP2" running on the IBM Z platform.

Original advisory:

SUSE-SU-2018:0012-1:
https://www.suse.com/support/update/announcement/2018/suse-su-20180012-1/
SUSE-SU-2018:0069-1:
https://www.suse.com/support/update/announcement/2018/suse-su-20180069-1/

References:

SA80732:
SA80732
SA80843:
SA80843
SA80680:
SA80680

Changelog:

2018-01-11: 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) 12 SP2". Added a link to the "Original Advisory" section. Updated the "Solution" section.
2018-01-04: Initial release