Security Advisory Report - OBSO-1202-01

CVE-2012-0056 - Linux Kernel Privilege Escalation Vulnerability

Creation Date: 2012-02-01
Last Update: 2013-11-08

Summary

A Linux Local Privilege Escalation vulnerability was published on January 17 and meanwhile associated exploit code is available in the public, too.

Vulnerability Details

The vulnerability affects systems with Linux Kernel versions 2.6.39 or higher. Exploiting this vulnerability allows local Linux users to gain full control with root (superuser) privileges on the system.

The OpenScale Baseline Security Office rates the risk for this type of vulnerability as low, provided that the appropriate hardening measures have been taken - see the section "Recommended Actions" for details.

Furthermore, no product of Unify is directly affected by this vulnerability - see the section "Affected Products" for details.

Affected Products

None.

All products of Unify are using Linux kernel versions (either native or based on a SuSE Linux distribution), which are not affected by this vulnerability.

Recommended Actions

No **specific actions** required for this vulnerability.

General recommendations:

Regardless of this particular Linux kernel vulnerability, we recommend in general, that your systems are appropriately hardened (which will also protect your solutions for similar - possibly still unknown - types of vulnerabilities):

- Disable all local Linux user accounts which are not relevant for the operation of the server
- Set appropriate individual and complex passwords for the remaining accounts
- Use SSHv2, and disable SSHv1 and telnet
- Ensure that only trusted persons have access to the local accounts of the servers

The relevant configuration steps are described in the product's individual Security Checklist (and/or Installation Manual).

References

- secunia.com/advisories/47378
- blog.zx2c4.com/749
- www.kb.cert.org/vuls/id/470151
- cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0056

Revision History

2012-02-01: Initial release
2013-11-08: Rereleased under the Unify brand (formerly Siemens Enterprise Communications)

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com