# Security Advisory Report - OBSO-1503-02

## Samba smbd - Remote Code Execution Vulnerability in netlogon server (CVE-2015-0240)

Creation Date: 2015-03-31
Last Update: 2015-03-31

## Summary

The smbd file server daemon of Samba (a file service solution for interoperability of Linux servers with Windows file systems) is vulnerable to remote code execution that may allow a remote attacker to execute arbitrary code on the Linux server with root privileges.

This advisory summarizes the impact of the vulnerability for customers using products of Unify and the recommended countermeasures.

**The risk is rated as high for older versions of OpenScape Business V1.**
Current versions of OpenScape Business V1, as well as **other products of Unify are not affected** by this vulnerability.

## Vulnerability Details

Samba is a freely available file and printer sharing application. Samba allows users to share files and printers between operating systems on Unix/Linux and Windows platforms and is part of most commonly known Linux distributions.

The smbd daemon is prone to a remote-code-execution vulnerability. An attacker can exploit this issue by sending specially-crafted netlogon packets that may allow arbitrary code execution with the privileges of the smbd process (on standard Linux installations these are typically root privileges, which can result in the complete compromise of affected systems that have enabled the smbd daemon).

The vulnerability is relevant to samba version 3.5.x and later, but does not exist in 3.4.x and earlier.
(--> therefore, for example Novell SLES versions 10 SP4 or 11 SP1 are not affected, while 11 SP2 and SP3 are).

**CVSS Scores:**

- CVSS Base Score: 10.0
- CVSS Temporal Score: 7.4
- CVSS v2 Vector (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)

## Affected Products

- **OpenScape Business V1: All versions before V1 R3.1.0 (release date: 2014-08-21)**
  are affected as a vulnerable smbd daemon was active and provided by default in this older versions. We recommend to upgrade to V1 R3.1.0 or any later version, where the Samba service was removed
- **OpenScape Office V3** is not vulnerable.
  Note however that all versions **before** V3 R3.11.0 (release date: 2014-10-17) provided the Samba service similar to OpenScape Business, but based on a non vulnerable version of the smbd daemon. Nevertheless, as a precautionary measure, we recommend to upgrade OpenScape Office to later versions to avoid potential future attack vectors associated with the Samba service.

**Other Unify products are not affected** as they do not use Samba or rely on it.
Therefore, for appliance-type products (such as OpenScape Voice, Branch, SBC or 4000), the service is either not installed or not active.
On Linux-based applications (such as OpenScape UC Application servers, OpenScape 4000 Manager or OpenScape Xpert MLC), the Samba service should not be active (per default Unify hardening recommendations).

## Recommended Actions

- **OpenScape Business V1**: upgrade to version V1 R3.1.0 (release date: 2014-08-21) or later
- **OpenScape Office V3** (not vulnerable, but recommended as precautionary measure): upgrade to V3 R3.11.0 (release date: 2014-10-17) or later

Novell SLES and Debian Linux based application servers: review the current settings of the Samba service:

- If active and not used: deactivate it.
- If active and used: apply the relevant patches provided by Novell / Debian as listed in the references section.

## References

External links:

- samba.org Security Advisory: https://www.samba.org/samba/security/CVE-2015-0240
- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0240
- NVD: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0240

Patch information for Operating Systems:

- Novell SLES: https://www.suse.com/security/cve/CVE-2015-0240.html
- Debian Linux: https://security-tracker.debian.org/tracker/CVE-2015-0240

## Revision History

2015-03-31: Initial release

---

Advisory ID: OBSO-1503-02 (a=105), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

**Contact and Disclaimer**
OpenScape Baseline Security Office
obso@unify.com

Hofmannstr. 63, D-81379 München
www.unify.com