Suchy MIPS
http://www.suchymips.de

## SECURITY SCAN OF THE BENS G4 PRINTSERVERS - INFORMATION SHEET

We - the company Suchy MIPS GmbH and manufacturer of the BENS G4 print server - take "Vulnerability Reports" very seriously and take immediate remedial action when real vulnerabilities arise and provide updates as quickly as possible.

If you would like to send us or our partners from whom you purchased the BENS G4 print server a scan report for comment, please make the following statements:

- Which program was used for scanning
- Which version of the scanning program was used
- Which program settings were used for the scan
- Which version of the BENS OS was scanned

Please understand that we cannot process your report without this information and therefore we will not be able to comment.

Please also make sure that the scan program settings are correct and appropriate before scanning. The scanner's standard settings are often incorrectly used. However, the standard settings mostly apply to publicly accessible web servers and therefore deliver inadequate "Vulnerability reports" related to the BENS G4 print server. Inappropriate, because the BENS print server is not a publicly accessible server, but an on-premise server that is used exclusively in-house and is behind a firewall. Different scan configuration rules apply to such servers than to publicly accessible servers, because there are also other risks here. With this information sheet we would like to give you tips and some explanations for the scan configuration in order to avoid misunderstandings and to enable you to carry out a practical security scan, on which it will be easy for us to comment. On request, we would be happy to assist you in configuring the scanning program.

**For scanner configuration**:

- Do not perform scans that only check the release no. of binaries, web servers and program modules. With this setting, the scanning programs get information about all releases of found programs from their own database and not from the examined systems. This means that they report vulnerabilities in program releases that may not be installed on the BENS G4 print server at all. The scanners also do not check whether the objects and modules found are used and often report vulnerabilities during the release scan, which in fact are not.

**Scanning without service users**

- We recommend a security scan without service users. In this case, the scanning program behaves like an actual intruder performing a port scan at the TCP / IP level to find out if there is an open port through which it could penetrate.

**Scan with service users**

- If required, we can create a service user on the BENS G4 print server after consultation with you. In this case, a scan is carried out "from the inside". Among other things, sending ports are also recorded, but unfortunately also programs that are supplied with the Linux distribution but are not used at all and therefore do not pose any real risk.

**Scanning / monitoring with an agent.**

- Most providers of scanning programs offer so-called "agents" that can be installed on servers. On request, we will install an appropriate agent on the BENS G4 print server - if this is possible - provided that the functions of the server are not affected. The agents report all required information about the server and the functions it uses in a predefined period of time. We support you in the configuration of all components to avoid misunderstandings in the case of non-real risks.

**Ports used by the BENS G4 print server.**

Please note that the BENS G4 print server has to use some ports in order to be able to perform its actual functions and must therefore keep it open. It may happen that some scanning programs report some of these ports as risk. A typical example is port 515, which is classified as a risk by several scanning programs. However, the LPD daemon works with this port, without which e.g. printing from an SAP system using access method "U" would not be possible.

**Here is the list of the ports currently used by the BENS G4 print server:**

| | |
|---|---|
| TCP 80 / 443- | Web Interface (HTTP/HTTPS and IPPS (Secure IPP) |
| TCP 9100-9999 | typical for socket printers |
| TCP 5001 – 5999 | IPDS printers |
| TCP 515 | LPR printers |
| TCP 631 | IPP printers |
| TCP 139 | SMB printers and netdisks |
| TCP 445 | SMB printers and netdisks |
| TCP 22 | master/slave synchronization, SFTP netdisks |
| TCP 25 | sending mails, SMTP printers |
| TCP 587 | sending mails, SMTP printers |
| TCP 110 | POP3 netdisks |
| TCP 995 | POP3 netdisks |
| TCP 20 | FTP netdisks |
| TCP 21 | FTP netdisks |
| UDP/TCP 123 | time synchronization (if NTP is enabled) |
| UDP/TCP 161/162 | monitoring printers via SNMP / SNMP Trap |
| ICMP echo | monitoring printers via ping |
| TCP 3306 | BENS Database (if it is in use) |