INFORMATIONSBLATT Z.T. "SICHERHEITSSCAN DES BENS G4 PRINTSERVERS"

Wir - die Firma Suchy MIPS GmbH, Hersteller des BENS G4 Printservers - nehmen "Schwachstellen-Reports" (engl. "Vulnerability Reports") sehr ernst und ergreifen beim Auftauchen von echten Schwachstellen sofort Abhilfemaßnahmen und stellen so kurzfristig, wie nur möglich, Updates zur Verfügung.

Wenn Sie uns bzw. unseren Partnern, bei denen Sie den BENS G4 Printserver erworben haben, einen Scan-Report zur Stellungnahme zukommen lassen möchten, machen Sie bitte unbedingt folgende Angaben:

- Mit welchem Programm wurde gescannt
- Welche Version des Scannprogramms wurde verwendet
- Welche Programmeinstellungen wurden beim Scann verwendet
- Welche Version vom BENS OS wurde gescannt

Bitte haben Sie Verständnis dafür, dass wir ohne diese Angaben Ihren Report nicht bearbeiten können und uns deshalb eine Stellungnahme nicht möglich sein wird.

Bitte achten Sie auch vor dem Scannen auf korrekte und angemessene Einstellungen des Scanprogramms. Oft werden die Standardeinstellungen der Scanner genutzt. Die Standardeinstellungen gelten aber meistens für öffentlich zugängliche Web-Server und liefern unangemessene Schwachstellen. Unangemessen, denn der BENS G4 Printserver ist kein öffentlich zugänglicher Server, sondern ein On-Premise Server, der ausschließlich in-house gebraucht wird und hinter einer Firewall steht. Für solche Server gelten andere Scann-Konfigurationsregeln als für öffentlich zugängliche Server, denn hier drohen nicht die gleichen Gefahren, wie bei öffentlich zugänglichen Servern.

Dieses Dokument informiert u.A. über die wichtigsten Ports, die auf dem BENS G4 Printserver standardmäßig genutzt werden.

Bitte beachten Sie, dass der BENS G4 Printserver einige Ports offen halten muss, um seine eigentlichen Funktionen ausführen zu können. Es kann vorkommen, dass manche Scannprogramme einige dieser Ports als Schwachstellen bzw. Risiko reporten. Ein typisches Beispiel ist der Port 515, der von etlichen Scanprogrammen als Risiko eingestuft wird. Mit diesem Port arbeitet aber der LPD-Dämon, ohne dem z.B. das Drucken aus einem SAP-System über Koppelart "U" gar nicht möglich wäre.

LISTE DER PORTS DIE AUF DEM BENS PRINTSERVER STANDARDMÄßIG OFFEN SIND.

PORT	Beschreibung	Wenn der Port geschlossen wird…
TCP 80	Web Interface HTTP	Wenn der Port geschlossen wird, dann kann das BENS WEB-Interface nur noch über HTTPS (Port 443) erreicht werden.
TCP 443	Web Interface HTTPS	Wenn der Port geschlossen wird, dann kann das BENS WEB-Interface nur noch über HTTP (Port 80) erreicht werden. Wenn sowohl Port 80 als auch Port 443 geschlossen werden, dann kann das BENS WEB-Interface nicht mehr erreicht werden. Der BENS Printserver ist dann nicht mehr administrierbar. Bei geschlossenen Ports 80 UND 443 können keine Ports mehr geöffnet werden.
TCP 9100-9999	typical for socket printers	Wenn der Port geschlossen wird, dann können keine Virtuellen Drucker vom Typ "SMB" mehr benutzt werden.
TCP 5001 – 5999	IPDS printers	Wenn diese Ports geschlossen werden, dann können keine IPDS-Drucker mehr benutzt werden.
TCP 515	LPR printers	Wenn dieser Port geschlossen wird, dann können keine virtuellen Drucker vom Typ "LPR" mehr benutzt werden.
TCP 631	IPP printers	Wenn dieser Port geschlossen wird, dann können keine virtuellen Drucker vom Typ "IPP" mehr genutzt werden.
TCP 139	SMB printers and netdisks	Wenn dieser Port geschlossen wird, dann können keine virtuellen Drucker vom Typ "SMB" und keine Netdisks mehr benutzt werden.
TCP 445	SMB printers and netdisks	Wenn dieser Port geschlossen wird, dann können keine virtuellen Drucker vom Typ "SMB" und keine Netdisks mehr benutzt werden.
TCP 22	master/slave synchronization, SFTP netdisks	Wenn dieser Port geschlossen wird, dann können a) keine Services am BENS OS mehr durchgeführt, b) keine Master/Slave Verbindungen konfiguriert und keine SFTP netdisks mehr betrieben werden.

TCP 25	sending mails, SMTP printers	Wenn dieser Port geschlossen wird, dann können keine E-Mails vom BENS Printserver mehr versendet werden.
TCP 587	sending mails, SMTP printers	Wenn dieser Port geschlossen wird, dann können keine E-Mails vom BENS Printserver mehr versendet werden.
TCP 110	POP3 netdisks	Wenn dieser Port geschlossen wird, dann können keine E-Mails vom BENS Printserver mehr versendet werden.
TCP 995	POP3 netdisks	Wenn dieser Port geschlossen wird, dann können keine E-Mails vom BENS Printserver mehr versendet werden.
TCP 20	FTP netdisks	Wenn dieser Port geschlossen wird, dann können keine FTP netdisks mehr benutzt werden
TCP 21	FTP netdisks	Wenn dieser Port geschlossen wird, dann können keine FTP netdisks mehr benutzt werden
UDP/TCP 123	time synchronization (if NTP is enabled)	Wenn dieser Port geschlossen wird, dann wird keine Zeitsynchronisation mit einem NTP Server stattfinden
UDP/TCP 161/162	monitoring printers via SNMP / SNMP Trap	Wenn dieser Port geschlossen wird, dann werden vom BENS Printserver keine SNMP Abfragen mehr beantwortet
ICMP echo	monitoring printers via ping	Wenn dieser Port geschlossen wird, dann antwortet der BENS Printserver auf PING nicht mehr
TCP 3306	BENS Database (if it is in use)	Wenn dieser Port geschlossen wird, dann kann die interne BENS Datenbank nicht mehr genutzt werden.
TCP 5500	IPDS / AFPDS Konverter	Wenn dieser Port geschlossen wird, dann kann das AFPDS/IPDS Plugin nicht mehr gestartet werden
TCP 7001	XML-RPC	Wenn dieser Port geschlossen wird, dann kann der BENS Printserver nicht mehr über das WEB-Interface erreicht werden und der Server ist nicht mehr administrierbar.

KOMMENTARE ZU PORTS, DIE VOM SCANPROGRAMM NESSUS ALS SCHWACHSTELLEN GEMELDET WERDEN.

41028 - SNMP Agent Default Community Name (public)

Das ist die Standardeinstellung. Der Name der SNMP Community kann geändert werden.
Benutzen Sie dazu den Eintrag
adv.snmp.server.community
im Modul Einstellungen / Erweitert.
Nach der Änderung müssen die Clients, die den Status von Virtuellen Druckern via SNMP abfragen so umkonfiguriert werden, dass sie den gleichen Community-Namen benutzen.

Zusätzlich kann der SNMP Server ganz abgeschaltet werden.
Benutzen Sie dazu den Eintrag
adv.snmp.server.enabled
im Modul Einstellungen / Erweitert
Nach der Abschaltung des SNMP Servers können keine SNMP Abfragen zum Status der Virtuellen Drucker mehr verarbeitet werden.

57582 - SSL Self-Signed Certificate
57582 - SSL Self-Signed Certificate
51192 - SSL Certificate Cannot Be Trusted
51192 - SSL Certificate Cannot Be Trusted

Diese Meldungen erscheinen aufgrund der selbst-signierten, internen Zertifikate von Suchy MIPS. Auf Wunsch können wir ein Upgrade mit einem kundeneigenen Zertifikat vorbereiten. Die Prozedur ist kostenpflichtig.

104743 - TLS Version 1.0 Protocol Detection

Diese Meldung wird von Linux Drucksystem CUPS verursacht. Wenn kein IPP-Protokoll genutzt wird, kann CUPS abgeschaltet werden.
Benutzen Sie dazu den Eintrag
adv.daemon.cups.enabled
im Modul Einstellungen / Erweitert

SCHLIEßUNG VON PORT

Wichtig: Ab OS Version 4.2.0-r21937 können nicht benötigte Ports vom BENS-Administrator gesperrt werden. Benutzen Sie dazu den Eintrag "**adv.firewall.deny**" im Modul Einstellung / Erweitert. Dort können mehrere Ports gleichzeitig, getrennt durch Komma, angeben werden, z.B. 80, 9100,... usw.

Wichtig: Gehen Sie sehr vorsichtig mit der Portsperrung um und prüfen die möglichen Konsequenzen, bevor Sie einen Port sperren. Mit nicht sachgemäßem Umgang mit der Portsperrung können Sie den BENS Printserver inoperabel und nicht administrierbar machen. In solchen Fällen müsste der BENS Server komplett neu installiert werden.