RELEASE NOTES SYSTEMSOFTWARE 7.1.15

Release Notes - Systemsoftware 7.1.15
Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.1.15**.

Haftung

Der Inhalt dieses Dokuments wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Dokument gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen finden Sie unter www.bintec.de.

Als Multiprotokoll-Gateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EC

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Neue Funktionen

Systemsoftware 7.1.15 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber Systemsoftware 7.1.14 erheblich erweitern:

1.1 Kostenfreie IPSec-Lizenz

Mit Systemsoftware 7.1.15 unterstützen Bintec Gateways entsprechend der Beschreibung im Bintec Benutzerhandbuch standardmäßig zwei aktive IPSec-Tunnel (für eine detaillierte Beschreibung siehe z. B. das X2250-Benutzerhandbuch).

Hinweis

Beachten Sie, dass die Lizenz nicht die Anzahl der auf dem Gateway konfigurierbaren Peers beschränkt, sondern lediglich die Anzahl der gleichzeitig aktiven IPSec-Verbindungen.

1.2 Neue Zeitsynchronisationsoptionen

Die Optionen für die Aktualisierung der Systemzeit des Gateways von verschiedenen Quellen wurden wesentlich erweitert, um mehrere Zeitserver konfigurieren zu können.

Das Menü für die Konfiguration der Zeitabfrageoptionen wurde erweitert, es wird über das ***System***-Menü aufgerufen (***System*** ‹ ***Time and Date***):

```
X2302 Setup Tool                     BinTec Access Networks GmbH
[SYSTEM][TIME]: Control System Time and Date                MyGateway

 Current System Time: Wed 2005/Feb/28 19:19:37  set by: None

 Change  System Time:     2005/Feb/28       19:19:17            CHANGE


Time Update Interval          :      86400     Seconds
Update System Time from ISDN :       disabled
System Time Offset from GMT   :      0         Seconds

Time Servers:

   Name/Address                                 Protocol
1:                                              SNTP
2:                                              SNTP
3:                                              SNTP

         SAVE                            CANCEL
```

Die erste Zeile im Menüfenster zeigt die aktuelle Systemzeit an. Diese kann manuell in der Sekundenzeile durch Editieren der Felder für Datum und Uhrzeit eingestellt werden. Durch Bestätigen mit ***CHANGE*** werden die Änderungen übernommen.

Da von einem Gateway ohne Hardware Real Time Clock (Liste der Gateways ohne Real Time Clock) die Systemzeit beim Neubooten zurückgesetzt wird, unterstützt die **Systemsoftware 7.1.15** die Synchronisation mit mehreren Zeitservern und über ISDN. Das Setup Tool ermöglicht die Konfiguration von drei Zeitservern, weitere können über die SNMP-Shell konfiguriert werden. Diese Optionen werden in der unteren Hälfte des Menüfensters konfiguriert. Das Menü bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
Time Update Interval	Hier geben Sie das Zeitintervall ein, in dem das Gateway versucht, sich auf einen der konfigurierten Zeitserver zu synchronisieren (in Sekunden). Der Standardwert ist *86400*.

Feld	Beschreibung
Update System Time from ISDN	Hier können Sie festlegen, ob die Zeitinformation, die am Ende eines ISDN-Rufs gesandt wird, zur Aktualisierung der Systemzeit benutzt wird. Diese Option wird nur solange genutzt, wie nach einem Neustart kein erfolgreiches Update von einem Zeitserver empfangen wurde Verfügbare Werte sind *enabled* (freigegeben) und *disabled* (gesperrt), der Standardwert ist *disabled*.
System Time Offset from GMT	Hier geben Sie die Abweichung zwischen der lokalen Uhrzeit und GMT ein. Die Werte werden in Sekunden eingegeben; Werte zwischen *1* und *23* werden jedoch als Stunden interpretiert und nach dem Speichern der Konfiguration in Sekunden umgewandelt. Es können positive oder negative Werte eingegeben werden, der Standardwert ist *0*.
Name/Address	Hier können Sie bis zu drei Zeitserver eingeben, entweder durch ihre Domainnamen oder durch ihre IP-Adresse. Es gibt keine vorkonfigurierten Server.

Feld	Beschreibung
Protocol	Hier können Sie das Protokoll auswählen, welches für die Abfrage der Zeitserver benutzt wird. Zur Auswahl stehen: ■ *SNTP* - Dieser Server nutzt das Simple Network Time Protocol. ■ *disabled* - Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt. ■ *TIME/UDP* - Dieser Server nutzt das Time/UDP-Protokoll. ■ *TIME/TCP* - Dieser Server nutzt das Time/TCP-Protokoll.

Tabelle 1-1: ***SYSTEM → TIME AND DATE***

Liste der Gateways ohne Real Time Clock

Die folgenden Gateways verfügen nicht über eine Real Time Clock:

- **X1000 II**
- **X1200 II**
- **X2250**
- **X2300** compact ab Seriennummer "X2C25...."
- **X2300s**
- **X2300i** compact ab Seriennummer "X2I25..."
- **X2300is** compact ab Seriennummer "X2Y25..."
- **X2404** compact ab Seriennummer "X2D21..."
- **X2500**
- **VPN Access 5**, **25** und **100**
- **X2301**
- **X2302**.

1.3 TACACS+

Das TACACS+ Protokoll ermöglicht die Zugriffssteuerung von Gateways, Netzzugangsservern (NAS) und anderen Netzwerkkomponenten über einen oder mehrere zentrale Server. TACACS+ bietet Authentifizierungs-, Autorisierungs- und Abrechnungsdienste.

Die Konfiguration eines TACACS+ Servers wird über das Menü ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***TACACS+ AUTHENTICATION AND AUTHORIZATION*** ➜ ***ADD/EDIT*** vorgenommen.

```
X2302 Setup Tool                        BinTec Access Networks GmbH
[IP][TACACS+][ADD]                                          MyGateway

  Server's IP Address or Hostname

  Priority                              0            TCP Port  49
  TACACS+ Key (Secret)
  Policy                                non authoritative
  Encryption (recommended)              enabled

  Timeout (seconds)                     3
  Block Time (seconds)                  60

  PPP Authentication                    disabled
  Login Authentication/Authorization    enabled
  TACACS+ Accounting                    disabled
  Administrative Status                 up
  TACACS+ Single-Connection             single request

                    SAVE                                CANCEL
```

Das Menü bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
Server's IP Address or Hostname	Hier geben Sie die IP-Adresse des TACACS+ Servers ein, der für eine AAA-Anforderung (Authentifizierung, Autorisierung, Abrechnung) abgefragt werden soll.

Feld	Beschreibung
Priority	Hier weisen Sie dem aktuellen TACACS+ Server eine Priorität zu. Der Server mit dem niedrigsten Wert ist der erste, der für die TACACS+ AAA-Anforderung benutzt wird. Falls er keine Antwort gibt oder der Zugriff verweigert wurde (nur im nichtautoritativen Fall, siehe auch das Feld ***POLICY***), wird der Eintrag mit der nächstniedrigeren Priorität genutzt. Verfügbare Werte sind *0* bis *9*, der Standardwert ist *0*.
TCP Port	Der für das TACACS+ Protokoll benutzte Standard-TCP-Port ist auf *49* eingestellt. Dieser Wert kann nicht verändert werden.
TACACS+ Key (Secret)	Hier geben Sie das Passwort ein, welches benutzt wird, um den Datenaustausch zwischen dem TACACS+ Server und dem Netzzugangsserver (Ihrem Gateway) zu authentifizieren und (falls zutreffend) zu verschlüsseln. Die maximale Länge des Eintrags ist 32 Zeichen.

Feld	Beschreibung
Policy	Hier können Sie die Interpretation der TACACS+ Antwort auswählen. Verfügbare Werte sind *authoritative* und *non authoritative*. Wenn in diesem Feld *authoritative* eingetragen ist, wird eine negative Antwort auf eine Anfrage akzeptiert. Dies ist nicht notwendigerweise der Fall, wenn die Einstellung *non authoritative* (Standardwert) lautet. In diesem Fall wird der nächste TACACS+ Server abgefragt, bis eine autoritative Antwort kommt. Ist ***POLICY*** auf *non authoritative* gesetzt und keiner der Server liefert eine positive Antwort, oder ist keiner der Server erreichbar, werden die lokal konfigurierten SNMP Communities auf passende Zugangsinformation überprüft.
Encryption (recommended)	Hier können Sie festlegen, ob der Datenaustausch zwischen dem TACACS+ Server und dem NAS verschlüsselt werden soll oder nicht. Verfügbare Werte sind *enabled* (Standardwert) und *disabled*. Falls *enabled* eingestellt wird, werden die TACACS+ Pakete mit MD5 verschlüsselt. Andernfalls - bei Einstellung auf *disabled* - werden die Pakete und damit alle dazugehörigen Informationen unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung empfohlen.

Feld	Beschreibung
Timeout (seconds)	Hier geben Sie die Zeit ein, wie lange der NAS auf eine Antwort von TACACS+ wartet. Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster konfigurierte TACACS+ Server abgefragt und der aktuelle Server in einen *blocked*-Status versetzt (***TACACSPSERVEROPERSTATUS*** = *blocked*). Verfügbare Werte sind *1* bis *60*, der Standardwert ist *3*.
Block Time (seconds)	Hier geben Sie die Zeit ein, wie lange der aktuelle Server in einem blockierten Status bleibt. Nach Ende der Blockierungsdauer wird der Server in den Status versetzt, der im Feld ***ADMINISTRATIVE STATUS*** angegeben ist (siehe unten). Verfügbare Werte sind *0* bis *3600*, der Standardwert ist *60*. Der Wert *0* bedeutet, dass der Server nie in einen *blocked*-Status versetzt wird.
PPP Authentication	Diese Funktion wird von der **Systemsoftware 7.1.15** nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert.
Login Authentication/Authorization	Hier können Sie festlegen, ob der aktuelle TACACS+ Server für die Login-Authentifizierung zu einem Gateway benutzt werden soll. Zur Auswahl stehen *enabled* (Standardwert) und *disabled*.
TACACS+ Accounting	Diese Funktion wird von der **Systemsoftware 7.1.15** nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert.

Feld	Beschreibung
Administrative Status	Hier können Sie den Status auswählen, in den der Server versetzt werden soll: falls die Einstellung *up* lautet, wird der dazugehörige Server für Authentifizierung, Autorisierung und Abrechnung gemäß Priorität (siehe Feld ***PRIORITY***) und aktuellem Betriebsstatus benutzt. Andernfalls wird dieser Eintrag für TACACS+ AAA-Anforderungen nicht berücksichtigt. Zur Auswahl stehen *up* (Standardwert) und *down*.
TACACS+ Single-Connection	Hier können Sie festlegen, ob mehrere TACACS+ Sitzungen (aufeinanderfolgende TACACS+ Anforderungen) gleichzeitig über eine einzige TCP-Verbindung unterstützt werden. Falls mehrere Sitzungen nicht über eine einzige TCP-Verbindung gemultiplext werden, wird für jede TACACS+ Sitzung eine neue Verbindung aufgebaut und am Ende der jeweiligen Sitzung abgebaut. Zur Auswahl stehen *multiple requests* und *single request* (*single request* ist Standardwert und wird für die meisten Anwendungen empfohlen).

Tabelle 1-2: ***IP ➜ REMOTE AUTHENTICATION (RADIUS/TACACS+) ➜ TACACS+ AUTHENTICATION AND AUTHORIZATION ➜ ADD/EDIT***

1.4 RADIUS

Systemsoftware 7.1.15 unterstützt RADIUS zum Zweck der Authentisierung, des Accountings, des IPSec Peer Retrievals und des Shell Logins gemäß der Beschreibung im Bintec Benutzerhandbuch (für eine detaillierte Beschreibung siehe z. B. das X2250-Benutzerhandbuch).

1.5 QoS

Systemsoftware 7.1.15 unterstützt QoS gemäß der Beschreibung im Bintec Benutzerhandbuch (für eine detaillierte Beschreibung siehe z. B. das X2250-Benutzerhandbuch).

1.6 "ifstat" für physikalische Interfaces

Der Befehl `ifstat` stand bisher nur für nicht physikalische Interfaces zur Verfügung. Systemsoftware 7.1.15 führt den ergänzenden Befehl `physifstat` ein, der entsprechende Funktionen auch für physikalische Interfaces zur Verfügung stellt.

Der Befehl wird folgendermaßen verwendet:

```
x2301:> physifstat -?
Usage:
        physifstat [ -lud ] [<interface>]
Options:
        -l              long interface names
        -u              only up interfaces
        -d              only down interfaces
Usage:
        physifstat <interface> up|down
             up: set <interface> to up
           down: set <interface> to down
x2301:>
```

Auf **X2301** und **X2302** stehen als Interfaces für diesen Befehl das Ethernet-Interface sowie das ATM-Interface zur Verfügung:

```
x2301:> physifstat -l
Index  Descr     Typ Speed  St Ipkts Ies Opkts Oes ChgTime
001000 XEY-100BT eth 100M   up 15561 5   77    0   0 00:00:00
003000 ar7sar-3  atm    0   dn 0     0   0     0   0 00:00:00
  total: 2
x2301:>
```

IES und ***OES*** stehen in der Tabelle für Incoming bzw. Outgoing errors, ***CHGTIME*** für den Zeitpunkt des letzten Statuswechsels.

Hinweis

Bitte beachten Sie, dass bei Ethernet-Interfaces immer nur das auf -0 endende Interface angezeigt wird, also z. B. en1-0. Virtuelle Interfaces (z. B. en1-0-1) werden nicht erfasst.

Darüber hinaus kann der operative Status eines Ethernet-interfaces nicht verändert werden.

1 Neue Funktionen

2 Änderungen

Folgende Änderungen wurden vorgenommen, um die Funktionalität Ihres Gateways zu erweitern:

2.1 PPTP - Zusätzliche konfigurierbare Parameter

Folgende für PPTP-Kontrollverbindungen relevante Parameter können ab **Systemsoftware 7.1.15** in der ***pptpProfileTable*** auf der SNMP Shell konfiguriert werden. Einträge in dieser Tabelle sind optional, und so lange keine expliziten Werte vorgegeben werden, werden systeminterne Defaultwerte verwendet.

- ***Host*** - Wird kein Wert für ***Host*** angegeben, wir der Wert der Variablen ***SysName*** aus der ***systemTable*** übertragen. Ansonsten wird der hier eingetragene Wert verwendet.
- ***Vendor*** **-** Wird kein Wert für ***Vendor*** angegeben, wird eine ID generiert, die sich aus "Bintec" und einem systeminternen Wert aus der ***biboAdmBoardTable*** zusammensetzt. Ansonsten wird der hier eingetragene Wert verwendet.
- ***FirmRev*** - Für ***FirmRev*** = *-1* wird die Firmware-Revision *0* übermittelt, für ***FirmRev*** = *0* (also auch, wenn kein Eintrag vorgenommen wird) wird die der Systemsoftware entsprechende Revision angegeben. Für jeden anderen Wert (*1* bis *999*) wird genau der eingegebene Wert übermittelt.

2.2 ATM - Standardprofil

Systemsoftware 7.1.15 enthält ein Standard-ATM-Profil, das die Konfiguration eines DSL-WAN-Partners vereinfacht.

Je nachdem, ob das Gateway an einem ADSL-über-POTS- oder ADSL-über-ISDN-Anschluss betrieben wird, findet sich im Menü ***ATM*** ➜ ***ETHERNET OVER ATM*** ein Standardprofil, das die Einstellungen für viele der angebotenen ADSL-Anschlüsse abbildet: Für ADSL über ISDN wird ein Eintrag mit ***VPI***=*1* und ***VCI***=*32* angelegt, für ADSL über POTS wird kein Eintrag angelegt.

2.3 Neue Option beim Setup-Tool-Start

Das Setup Tool kann unter **Systemsoftware 7.1.15** mit der Option `-I` gestartet werden. Diese Option startet das Setup Tool im Menü ***MONITORING AND DEBUGGING*** ➜ ***INTERFACES*** und gestattet keinen Zugriff auf andere Menüs des Setup Tools.

2.4 Neuer DHCP-Parameter

Mittels der neuen MIB-Variablen ***IPDHCPUSEDEFAULTHOSTNAME*** ist es möglich, festzulegen, ob das Gateway in einer DHCP Reply einen Standard-Host-Namen überträgt oder nicht. Ist für ***IPDHCPUSEDEFAULTHOSTNAME*** *disabled* ausgewählt wir kein Hostname übertragen, ist *enabled* ausgewählt, so wird ein vom Gateway aus der IP-Adresse des Clients generierter Host-Name übertragen. Der Defaultwert ist *enabled*.

3 Behobene Fehler

Folgende Probleme, die bei früheren Versionen unserer Systemsoftware auftreten konnten, wurden mit der Systemsoftware 7.1.15 gelöst:

3.1 SNMP Shell - Keine Syslog-Ausgabe mit "message"

(ID n/a)

Die Eingabe von `message` in der SNMP Shell sollte eigentlich zur Ausgabe der gesammelten Syslog-Meldungen führen, führte aber zur Darstellung einer MIB-Tabelle.

Das Problem ist gelöst worden.

3.2 MIB - Speicherverlust

(ID 3144)

Stagnierende Prozesse konnten auf dem Gateway zu einem Speicherverlust führen.

Das Problem ist gelöst worden.

3.3 DNS - Unerwünschte Namen im Cache

(ID 3364)

Gelegentlich wurde vom DNS Proxy nur der Fully Qualified Domain Name (FQDN, z. B. moon8.bintec.de) gespeichert, nicht aber der Canonical Name (CNAME, z. B. www.bintec.de).

Das Problem ist gelöst worden.

3.4 Setup Tool - Verwendung von „_“ nicht möglich

(ID 3619)

Wenn man in einem der DynDNS-Menüs einen Hostnamen eingab, so war die Verwendung von „_“ (Unterstrich) nicht möglich, obwohl es sich um ein für FQDNs akzeptables Zeichen handelt.

Das Problem ist gelöst worden.

3.5 HTML Wizard - Broadcasts durch Access Filter blockiert

(ID 3654)

Die IP Access Lists, die vom HTML Wizard erstellt wurden, blockierten Broadcasts auf dem WAN Interface. Das konnte zu Problemen führen, wenn das Gateway seine IP-Konfiguration per DHCP beziehen sollte.

Das Problem ist gelöst worden.

3.6 DHCP - Neustart

(ID 3670)

Es konnte bei der Bearbeitung eines DHCP Renew Requests zu einem Neustart des Gateways kommen.

Das Problem ist gelöst worden.

3.7 ARP - Falscher ARP Tell

(ID 3671)

Wenn ein Gateway über mehrere Interfaces verfügte (z. B. ein physikalisches und ein virtuelles), konnte es zu falschen ARP Tells kommen, bei denen die IP-Adresse des einen und die MAC-Adresse des anderen Interfaces verwendet wurden.

Das Problem ist gelöst worden.

3.8 Event Scheduler - Geringfügige Probleme

(ID 3679)

Die Implementierung des Event Scheduler wies einige kleinere Fehler auf:

- einen Schreibfehler („dayly“ anstatt „daily“);
- für ***SCHEDULE COMMANDS → ADD: INTERFACE*** war es bei der Konfiguration eines interface-spezifischen Befehls nicht möglich, ein WAN Interface auszuwählen;
- der Wert für ***BIBOEXTADMSCHEDULEINTERVAL*** wurde zurückgesetzt, wenn die Scheduler-Konfiguration mit dem Setup Tool durchgeführt wurde;
- es fehlte eine „Monday to Friday“-Bedingung für Scheduled Events.

Die Probleme sind gelöst worden.

3.9 Setup Tool - Load-Balancing-Konfiguration falsch gesichert

(ID 3680)

Bei der Konfiguration von ***IP Load Balancing over Multiple Interfaces*** mit ***Distribution Policy*** = *service/source-based routing* wurden falsche Werte in die ***ipExtRtTable*** geschrieben. Das konnte zu einer Fehlfunktion des Load Balancings führen.

Das Problem ist gelöst worden.

3.10 Setup Tool - X.25-Monitoring-Menü entfernt

(ID 3696)

Das Menü ***X.25 Monitoring*** war im Setup Tool vorhanden, obwohl **X2301** und **X2302** X.25 nicht unterstützen.

Das Problem ist gelöst worden.

3.11 PPPoE - Problem mit mehreren PPP Access Servern

(ID 3698)

Wenn ein Gateway so konfiguriert wurde, dass es zwei PPPoE Access Server nutzte, konnte der PPP Layer nicht aufgebaut werden.

Das Problem ist gelöst worden.

3.12 Setup Tool - Irrelevanter Menüpunkt entfernt

(ID 3703)

Das Setup Tool von **X2301** und **X2302** wies die Menüs zur Konfiguration des Bandwidth on Demand auf. Hierbei handelt es sich um eine nicht unterstützte Funktion.

Das Problem ist gelöst worden.

3.13 Setup Tool - IP-Accounting-Informationen falsch

(ID 3737)

Das Menü ***MONITORING AND DEBUGGING*** ➜ ***INTERFACES*** ➜ ***EXTENDED*** zeigte einen falschen Wert für ***SRCPRT*** an.

Das Problem ist gelöst worden.

3.14 PPPoE - Verbindungsaufbau erfolglos

(ID 3756)

Wegen eines zu kurzen Timeouts konnten bestimmte Arten von PPPoE-Verbindungen (z. B. Funkverbindungen) nicht hergestellt werden.

Das Problem ist gelöst worden.

3.15 ADSL - Kein Datenverkehr

(ID 3761)

Es konnte vorkommen, dass kein Datenverkehr über das ADSL-Interface möglich war. Gleichzeitig waren die Reaktionszeiten auf der SNMP Shell sehr lang.

Das Problem ist gelöst worden.

3.16 DNS - Erste DNS-Auflösung erfolglos

(ID 3809)

Nach der Erstkonfiguration eines Gateways im Auslieferungszustand kam keine Verbindung mit dem Internet zustande, weil für eine erste DNS-Auflösung keine Verbindung aufgebaut wurde.

Das Problem ist gelöst worden.

3 Behobene Fehler