AVM Technical Note

Session IDs und geändertes Login-Verfahren im FRITZ!Box Webinterface

Ab der FRITZ!Box Firmware-Version xx.04.74 wurde der vorhandenen Kennwortschutz verbessert sowie ein weiteres Sicherheitsmerkmal für den Zugriff auf die Konfigurationsoberfläche der FRITZ!Box eingeführt, die Session-IDs.

Die Verwendung von Session-IDs bietet einen wirksamen Schutz vor sogenannten Cross-Site Request Forgery Angriffen, bei denen ein Angreifer unberechtigt Daten in einer Webanwendung verändert. Das folgende Dokument beschäftigt sich mit der Verwendung von Session-IDs und richtet sich an Entwickler, die Tools für die FRITZ!Box programmieren.

Schutz vor Missbrauch

Neben der reinen Verwendung von Session-IDs läuft ein aktiver Schutz gegen mögliche Angriffsversuche. Versucht eine Anwendung ohne oder mit einer ungültigen Session-ID auf die FRITZ!Box zuzugreifen, werden alle aktiven Sitzungen aus Sicherheitsgründen beendet. Ein Zugriff auf die FRITZ!Box ist somit erst nach erneuter Anmeldung möglich.

Greift ein im Hintergrund laufendes Programm wie z.B. ein Anrufmonitor ohne gültige Session-ID permanent auf die FRITZ!Box zu, beendet dieser Zugriff eine aktive Sitzung. In der Praxis äußert sich das darin, dass die FRITZ!Box regelmäßig ein erneutes Login fordert.

Alle Programme, die auf das FRITZ!Box Webinterface zugreifen, sollten daher Session-IDs unterstützen, da sie sonst nicht nur keinen Zugriff mehr erhalten, sondern wie oben beschrieben auch den normalen Zugriff auf die FRITZ!Box Oberfläche über den Browser beeinträchtigen können.

Session ID-Verfahren

Verwendung der Session-ID

Die Session-ID ist eine 64Bit-Zahl, die durch 16 Hexziffern dargestellt wird. Sie wird beim Login vergeben und muss für die Dauer der Sitzung mitgeführt werden. Dabei sollte ein Programm zu jeder FRITZ!Box jeweils nur eine Session-ID verwenden, da die Anzahl der Sessions zu einer FRITZ!Box beschränkt sind.

Die Session-ID hat nach Vergabe eine Gültigkeit von 10 Minuten. Die Gültigkeitsdauer verlängert sich automatisch bei aktivem Zugriff auf die FRITZ!Box. Die Session-ID 0 (0000000000000000) ist immer ungültig.

Da die Verwendung der Session-IDs ein neues Feature ist, das per Firmwareupdate installiert wird, unterstützen nicht alle FRITZ!Boxen dieses Verfahren. Session-IDs müssen daher *zusätzlich* zu dem herkömmlichen Verfahren implementiert werden und parallel zu diesem laufen.

Vergabe der Session-ID

Für die Vergabe der Session-ID wurde eine neue Einstiegsseite *login_sid.xml* eingeführt.

Auf dieser Seite kann über den Wert <iswriteaccess> das Loginverfahren abgefragt werden. Beträgt der Wert 0, muss ein Login mit Kennwort erfolgen. Der dabei angewandte neue Login-Mechanismus wird weiter unten beschrieben.

Beträgt der Wert 1, ist kein Login erforderlich und es wird bei der Anfrage mit <SID> gleich eine gültige Session-ID mitgeteilt.

Sollte die Seite nicht aufgerufen werden können, handelt es sich um eine Firmware die keine Session-IDs unterstützt.

Übergabe der Session-ID

Die Übergabe der Session-ID erfolgt im Parameter **sid** (per GET oder POST).

Beispiel HTML-Formular:

```
<form action="…/cgi-bin/webcm" …>
…
<input type="hidden" name="sid" value="0000000000000001">
```

Beispiel für direkten Link:

```
<A HREF="…/cgi-bin/webcm?getpage=../html/seite.html&
    sid=0000000000000001</A>
```

Zugriff ohne Session-ID

Grundsätzlich können alle dynamisch generierten Seiten nur mit einer gültigen Session-ID aufgerufen werden. Auch das Lesen oder Schreiben von Web-Variablen erfordert eine Session-ID. Folgende Inhalte können ohne gültige Session-ID aufgerufen werden:

- Einstiegsseiten (z.B. Login-Seite)
- Statische Inhalte (z.B. Grafiken)

Beendung einer Sitzung

Eine Sitzung kann durch löschen der Session-ID jederzeit auch vor Ablauf des Timeouts von 10 Minuten beendet werden. Dies geschieht durch POST der Werte

```
sid=<Session-ID>
```

und

```
security:command/logout=<dummy>
```

wobei der Wert für <dummy> irrelevant ist.

Verändertes Login-Verfahren

Verwendet eine FRITZ!Box Session-IDs, erfolgt das Login nicht direkt über das Kennwort, sondern über einen Response-Wert, der aus dem Klartextkennwort und einer Challenge ermittelt wird.

Der Login-Vorgang sieht wie folgt aus:

```
<form action="../cgi-bin/webcm/" …>
…
<input type="password" name="login:command/response"
value="response">
</form>
```

Im Vergleich dazu der Login-Vorgang, wenn die FRITZ!Box noch keine Session-IDs unterstützt:

```
<form action="../cgi-bin/webcm/" …>
…
<input type="password" name="login:command/password"
     value="geheim">
</form>
```

Ermittlung des Response-Wertes

Beim neuen Login-Verfahren wird also das Klartextpasswort

```
login:command/password=<klartextpassword>
```

ersetzt durch

```
login:command/response=<response>
```

Der Response-Wert wird wie folgt gebildet:

```
<response> = <challenge>-<md5>
```

Der Wert <challenge> kann aus der Datei *login_sid.xml* ausgelesen werden
und <md5> ist der MD5 (32 Hex Zeichen mit Kleinbuchstaben) von

```
<challenge>-<klartextpassword>
```

Der MD5-Hash wird über die Bytefolge der UTF-16LE Codierung dieses Strings gebildet (ohne BOM und ohne abschließende 0-Bytes).

Aus Kompatibilitätsgründen muss für jedes Zeichen, dessen Unicode Codepoint > 255 ist, die Codierung des "."-Zeichens benutzt werden (0x2e 0x00 in UTF-16LE). Dies betrifft also alle Zeichen, die nicht in ISO-8859-1 dargestellt werden können, z.B. das Euro-Zeichen.

Abschließend ein Beispiel mit deutschem Umlaut:

Die Challenge

```
<challenge> = "1234567z"
```

kombiniert mit dem Kennwort

```
<klartextpassword> = "äbc"
```

ergibt den Wert

```
<response> = "1234567z-9e224a41eeefa284df7bb0f26c2913e2"
```