Link: https://www.computerwoche.de/a/microsoft-warnt-vor-luecke-in-asp-net,2354166

**IT-Sicherheit**

# Microsoft warnt vor Lücke in ASP.NET

**Datum: 23.09.2010**

**In einer Security-Meldung warnt Microsoft vor einer Schwachstelle im ASP.NET-Framework. Diese ermöglicht das Entziffern verschlüsselt übertragender Daten ohne Kenntnis des Schlüssels.**

Microsofts ASP.NET-Framework kommt bei vielen Websites für die Erstellung von Web-Anwendungen zum Einsatz. Sicherheitsforscher haben entdeckt, dass ASP.NET ebenso wie das Framework JavaServer Faces (JSF) anfällig für so genannte Padding-Oracle-Attacken ist. Damit können verschlüsselte Sitzungsdaten entziffert werden.

Die Sicherheitsforscher Juliano Rizzo und Thai Duong hatten eine solche Lücke bereits im Juni in JSF entdeckt und veröffentlicht. Auf der **Sicherheitskonferenz Ekoparty**[1] in Buenos Aires (Argentinien) haben sie vorgeführt, wie sich Sitzungsdaten, etwa Session-Cookies, von ASP.NET-Anwendungen mit selbst erstellten Tickets entziffern lassen.

Microsoft hat die **Sicherheitsmitteilung 2416728**[2] veröffentlicht, in der es vor der Schwachstelle in ASP.NET warnt und Möglichkeiten aufzeigt sie zu umschiffen. Zwar seien bislang keine realen Angriffen bekannt, doch sollten Administratoren prüfen, ob ihre Anwendungen anfällig für Padding-Oracle-Angriffe sind. Dazu stellt Microsoft ein Script bereit.

Kevin Brown erläutert im **Microsoft Security Research & Defense Blog**[3], wie mögliche Angriffe sowie die vorgeschlagenen Workarounds funktionieren. Ein "Padding Oracle" hat nichts mit dem Datenbankhersteller Oracle zu tun. Vielmehr handelt es sich um ein kryptografisches Orakel, also um ein System, das Hinweise gibt, wenn man Fragen an das System richtet. Im Fall von ASP.NET weist es einen Fehler auf, der es einem Angreifer ermöglicht durch gezielt Anfragen den Verschlüsselungs-Code zu ermitteln.

Der von Microsoft vorgeschlagene Workaround besteht letztlich darin dem Orakel den Mund zu verbieten, sodass es einem Angreifer keine Hinweise mehr liefert. Ob oder wann Microsoft ein Sicherheits-Update für ASP.NET bereit stellt, lässt der Hersteller einstweilen noch offen - die Untersuchungen seien noch nicht abgeschlossen. (**PC-Welt**[4]/wh)

## Links im Artikel:

[1] **http://ekoparty.org/**
[2] **http://www.microsoft.com/technet/security/advisory/2416728.mspx**
[3] **http://blogs.technet.com/b/srd/**
[4] **http://www.pcwelt.de/**