Kritisches Sicherheitsupdate: Spectre und Meltdown

Prozessoren verschiedener Hersteller weisen gravierende und schwer zu behebende Sicherheitslücken auf, wie Sicherheitsforsche von Google Project Zero und der Technischen Universität Graz aufgezeigt haben. Die gefundenen Schwachstellen, die als "Spectre" und "Meltdown" bezeichnet werden, ermöglichen das Auslesen von sensiblen Speicherinhalten des Computers. Das Bundesamt für Sicherheit in der Informationstechnik rat zwingend dazu das Sicherheitsupdate umgehend zu installieren.

Wie können Systeme kurzfristig geschützt werden?

Das Bundesamt für Sicherheit in der Informationstechnik bietet in Zusammenarbeit mit den Chipherstellern Intel und AMD eine schnelle Softwarelösung an, um die Lücken vor externen Missbrauch zu schützen. Für die meisten Einsatzszenarien auf einem PC oder Smartphone schließt das Sicherheitsupdate alle kritischen Lücken. Es ist zwingend notwendig, dieses Update zu installieren, um weiterhin Ihr Endgerät vor externen Angriffen zu schützen.

Updates zum Schließen der Lücken:

Das Sicherheitsupdate sollte umgehend auf allen normalen PCs installiert werden. Alle gängigen Windows Betriebssysteme werden unterstützt.

Microsoft Windows:

Bitte laden Sie sofort das Sicherheitsupdate herunter und installieren Sie dieses:

Link zum Herunterladen: **Hier**

Die Installation findet im Hintergrund statt und schließt umgehend alle beschriebenen Lücken

Unter Umständen kann es vorkommen, dass verschiedenen Antivirenprogramme fälschlicherweise ausschlagen, dies resultiert dadurch, dass das Sicherheitsupdate Lücken innerhalb der Prozessoren Architektur schließt. Wir raten dazu Ihr Antivirenprogramm für das Update kurzzeitig zu pausieren!

Inhaltsverzeichnis