CSCC Case der Woche

2015-01-02: Google veröffentlicht Zeroday für Windows

Titel **Google veröffentlicht Zeroday für Windows**	Risiko □■■■■
Betroffene Systeme:	Windows 8.1
Sachstand:	Seit Windows Vista dient die „User Access Control (UAC)“ dazu, einem dazu berechtigten Benutzer zeitweise höhere Privilegien unter Windows zu gewähren, beispielsweise zur Installation von Software oder für Anpassungen im System. Dazu wird eine modale Dialogbox eingeblendet, die Art und Umfang der erweiterten Rechte festlegt. In Windows 8.1 wurde durch das Google Project Zero eine Lücke entdeckt, die einem Prozess erlaubt, höher privilegierte Funktionen ohne vorherige UAC-Abfrage auszuführen.[1]
Bewertung:	Ein Angreifer oder eine Malware kann die beschriebene Schwachstelle ausnutzen. Durch die derzeit noch geringe Verbreitung von Windows 8.1 im Firmenumfeld kann jedoch von einer mittleren Gefährdung ausgegangen werden.
Empfehlung:	Der beschriebene Angriff kann verhindert werden, indem die Benutzerkontensteuerung im Systemmanagementcenter auf die höchste Stufe gesetzt wird. Dies kann manuell oder über entsprechende Gruppenrichtlinien erfolgen.
Quellen:	[1] Meldung bei Google Project Zero
Point of Contact	Dominik Neubauer, dne@it-tuv.com, 0221/969789-82

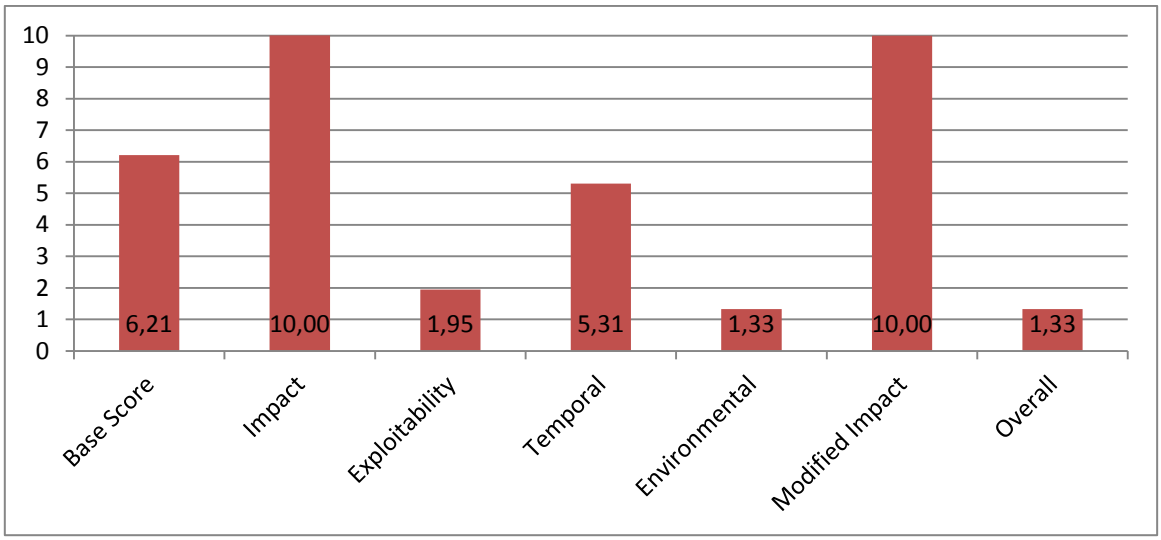

Abbildung 1: CVSS-Score zu Googles Zeroday in Windows 8.1