# Rahmenplan zur wöchentlichen CSCC-Telefonkonferenz

| Termin | Inhalt | Verantwortlich |
|---|---|---|
| bis Do 12:00 | Meldung von Sicherheitsvorfällen der vorigen Woche an TÜV TRUST IT[1] | CSCC-Mitglieder |
| bis Do 18:00 | Aufbereitung und Konsolidierung der gemeldeten Sicherheitsvorfälle | TÜV TRUST IT |
| bis Fr 09:30 | Einstellen eines neuen Sicherheitscodes im Telefonkonferenzportal für die Konferenz CSCC, im Reiter „Erweiterte Einstellungen“<br>Versand der Einwahldaten und ggf. Hintergrund-informationen | TÜV TRUST IT |
| Fr 10:00–12:00 | CSCC-Telefonkonferenz<br>Einwahl: ..... +49 69 2108 69 700<br>Teilnehmercode: (wird am Vormittag verschickt) | alle |
| Fr 12:00–14:00 | Möglichkeit für individuelle telefonische Beratung bzw. Nachfragen | TÜV TRUST IT |
| Anschließend (Fr. oder Mo.) | Zusendung des Berichts und des Protokolls an die CSCC-Mitglieder | TÜV TRUST IT |

[1] S/MIME- oder GnuPG-verschlüsselt an cscc@it-tuv.com
S/MIME-Fingerprint: f9f2f5bd 03f82916 7244a759 8fa542e6 38a22780
GnuPG-KeyID: 759B ABB7 21E6 A0F5 5E2F FDC0 0D09 E091 2F9E 3E57

# Agenda zur wöchentlichen CSCC-Telefonkonferenz

Einwahl: .....+49 69 2108 69 700

Admincode: .....[über das Konferenzportal erstellt und bis 09:30h versandt]

Teilnehmercode:.[über das Konferenzportal erstellt und bis 09:30h versandt]

PIN: .....[entfällt]

| TOP | Inhalt | Verantwortlich |
|---|---|---|
| 0 | Begrüßung, Vollzähligkeit<br>ggf. Vorstellung neuer Teilnehmer | TÜV TRUST IT |
| 1 | Offene Punkte der Vorwoche<br>Sofern aus vergangenen Telefonkonferenzen noch offene Punkte zur Klärung vorliegen, werden diese hier besprochen. | TÜV TRUST IT |
| 2 | TÜV Case der Woche<br>Eine aktuelle Entwicklung aus dem Umfeld der IT-Sicherheit wird vorgestellt, Hintergründe und Zusammenhänge erläutert und Auswirkungen und mögliche Mitigationsstrategien gegeben. | TÜV TRUST IT |
| 3 | Aktuelle Sicherheitslage<br>Die wesentlichen, seit der letzten Telefonkonferenz aufgetretenen externen Ereignisse mit Bezug zur IT-Sicherheitslage werden kurz vorgestellt, im Hinblick auf ihre Relevanz bewertet und erste resultierende Handlungsempfehlungen für die CSCC-Teilnehmer ausgesprochen. | TÜV TRUST IT |
| 4 | Auswertung gemeldeter Sicherheitsvorfälle<br>Die in der vergangenen Woche aufgetretenen Sicherheitsvorfälle werden in anonymisierter und konsolidierter Form vorgestellt und erste resultierende Handlungsempfehlungen für die CSCC-Teilnehmer ausgesprochen | TÜV TRUST IT<br>sowie ggf. weitere Experten |
| 5 | Diskussion und Rückfragen<br>Beantwortung bzw. Sammlung weiterer Rückfragen | alle |

Im Nachgang zur wöchentlichen Telefonkonferenz besteht die Möglichkeit, individuelle Rücksprache zu Sicherheitsthemen in individuellen Telefonterminen wahrzunehmen.

# CSCC Case der Woche

## 2015-01-02: Google veröffentlicht Zeroday für Windows

| Titel<br>**Google veröffentlicht Zeroday für Windows** | Risiko<br>□■■■■ |
|---|---|
| **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.<br>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 |

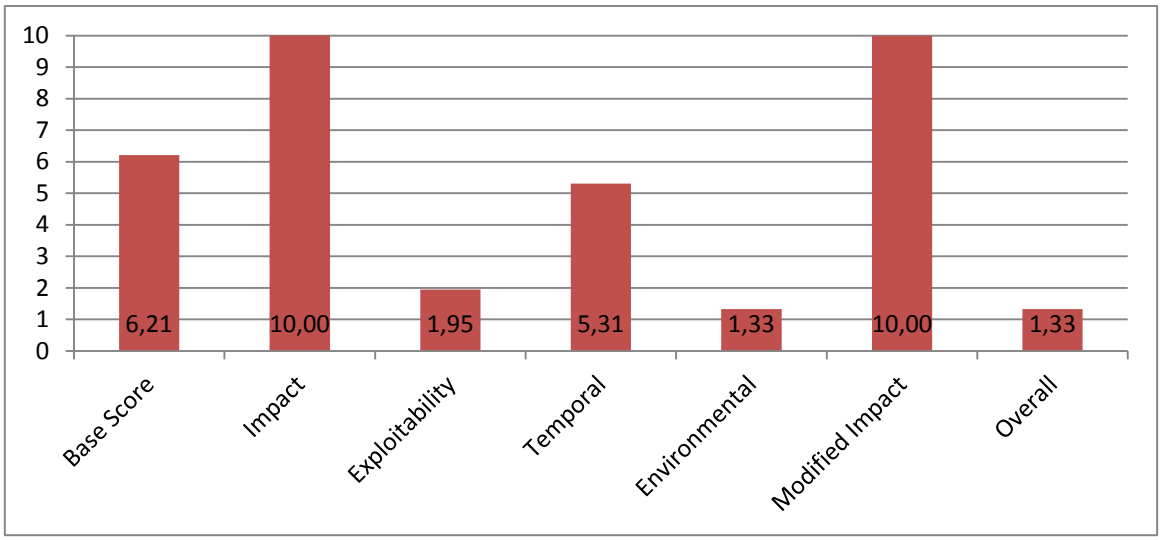


**Abbildung 1: CVSS-Score zu Googles Zeroday in Windows 8.1**

# 2015-01-13: Mainstream-Support für Windows 7 endet

| Titel<br>**Mainstream-Support für Windows 7 endet** | Risiko<br>**informativ** |
|---|---|
| **Betroffene Systeme:** | Windows 7 |
| **Sachstand:** | Windows 7 wurde im Oktober 2009 veröffentlicht, ab dann begann die Mainstream- und die Extended-Support-Phase mit einer Dauer von jeweils 5 Jahren.[1]<br>Der Mainstream-Support endet am 13. Januar 2015, der Extended Support läuft bis zum 14. Januar 2020. |
| **Bewertung:** | In der Extended-Support-Phase werden nur noch sicherheitskritische Patches veröffentlicht; für den Erhalt sonstiger Patches muss ein separater Supportvertrag abgeschlossen werden.[2] |
| **Empfehlung:** | Da das Ende des Mainstream-Supports keine unmittelbar sicherheits-relevanten Auswirkungen hat, wird keine explizite Handlungsempfehlung gegeben. |
| **Quellen:** | [1] Lifecycle Windows 7<br>[2] Microsoft Support Lifecycle-Richtlinie |
| **Point of Contact** | Dominik Neubauer, dne@it-tuv.com, 0221/969789-82 |

## Informationsquellen

Für die Erstellung des wöchentlichen Lagebilds werden Informationen über Schwachstellen aus öffentlichen und nicht-öffentlichen Quellen gesammelt, konsolidiert und für die Gesamtlage aufbereitet. Genutzte Quellen sind unter anderem:

- NIST[2] National Vulnerability Database (https://nvd.nist.gov/Home/Email-List)
- Alerts/Bulletins des US-CERT (https://www.us-cert.gov/)
- CERT-Bund Advisories (https://www.cert-bund.de/)
- Security-Mails des RUS-CERT (http://cert.uni-stuttgart.de/)
- Hinweise des Bürger-CERT (https://www.buerger-cert.de/)
- Sicherheitsmeldungen der CSCC-Teilnehmer
- Erkenntnisse aus Penetrationstests und Sicherheitsanalysen der TÜV TRUST IT
- Sonstige öffentliche und nicht-öffentliche Quellen zur IT-Sicherheitslage

Die im Verlauf der Woche gemeldeten Sicherheitsinformationen werden in Top 2 der wöchentlichen Telefonkonferenz vorgestellt.

[2] National Institute of Standards and Technology