Rahmenplan zur wöchentlichen CSCC-Telefonkonferenz

Termin	Inhalt	Verantwortlich
bis Mi 12:00	Meldung von Sicherheitsvorfällen der vorigen Woche an TÜV TRUST IT[1]	CSCC-Mitglieder
bis Mi 18:00	Aufbereitung und Konsolidierung der gemeldeten Sicherheitsvorfälle	TÜV TRUST IT
bis Do 11:00	Einstellen eines neuen Sicherheitscodes im Telefonkonferenzportal für die Konferenz CSCC, im Reiter „Erweiterte Einstellungen“ Versand der Einwahldaten und ggf. Hintergrund-informationen	TÜV TRUST IT
Do 13:00–15:00	CSCC-Telefonkonferenz Einwahl: ..... +49 69 2108 69 700 Teilnehmercode: (wird am Vormittag verschickt) PIN: ..... (wird am Vormittag verschickt)	alle
Do 15:00–17:00	Möglichkeit für individuelle telefonische Beratung bzw. Nachfragen	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 11:00h versandt]

Teilnehmercode:.[über das Konferenzportal erstellt und bis 11:00h versandt]

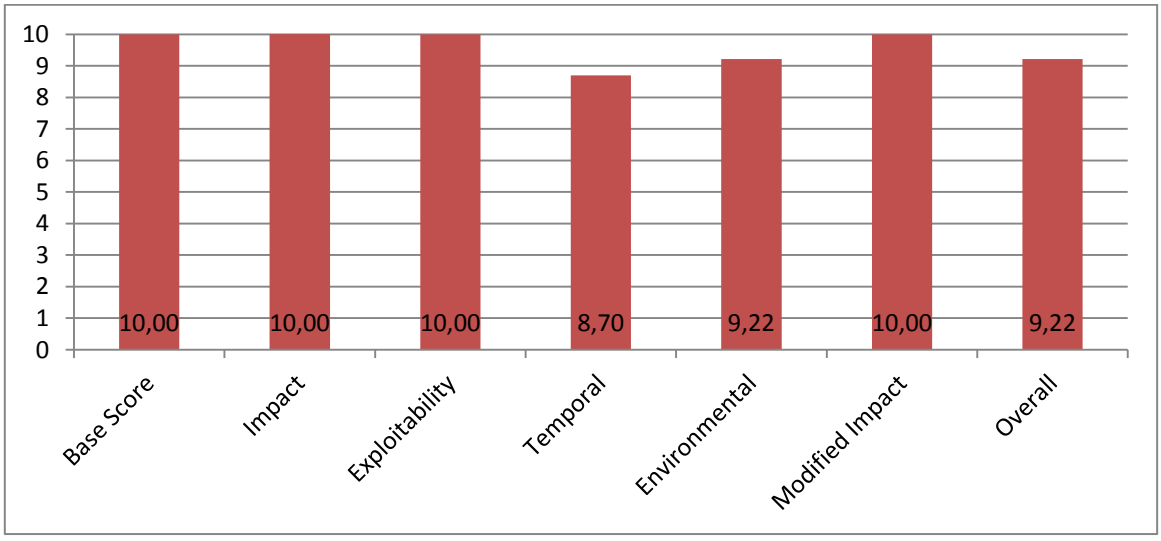
PIN: .....[über das Konferenzportal erstellt und bis 11:00h versandt]

TOP	Inhalt	Verantwortlich
0	Begrüßung, Vollzähligkeit ggf. Vorstellung neuer Teilnehmer	TÜV TRUST IT
1	Offene Punkte der Vorwoche Sofern aus vergangenen Telefonkonferenzen noch offene Punkte zur Klärung vorliegen, werden diese hier besprochen.	TÜV TRUST IT
2	Aktuelle Sicherheitslage 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
3	Auswertung gemeldeter Sicherheitsvorfälle 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 sowie ggf. weitere Experten
4	TÜV Case der Woche Eine aktuelle Entwicklung aus dem Umfeld der IT-Sicherheit wird vorgestellt, Hintergründe und Zusammenhänge erläutert und Auswirkungen und mögliche Mitigationsstrategien gegeben.	TÜV TRUST IT
5	Diskussion und Rückfragen Beantwortung bzw. Sammlung weiterer Rückfragen	alle

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

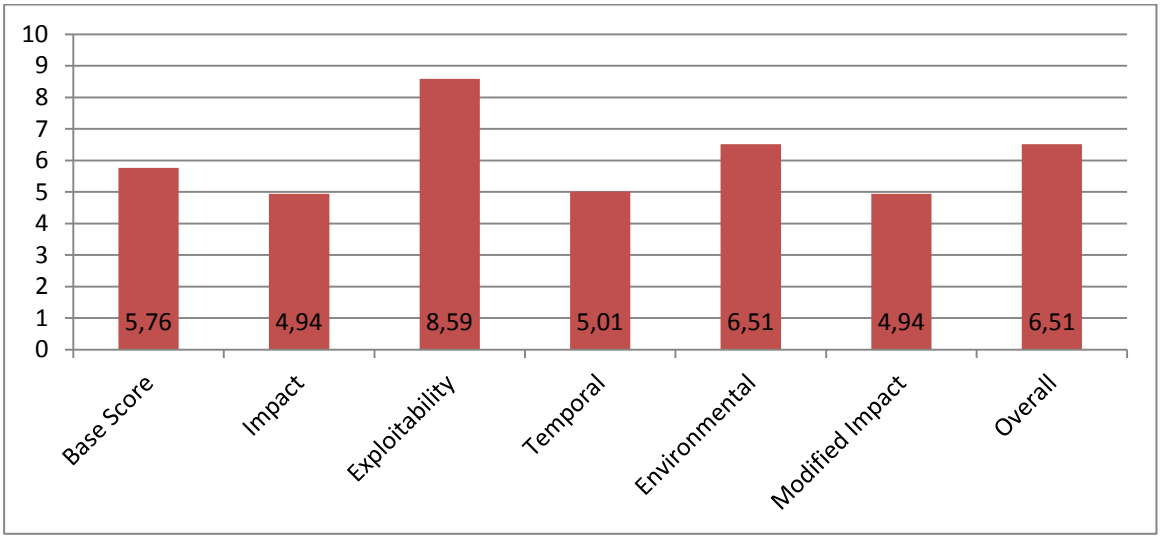
2014-09-04: Remote Code Execution in Google Chrome

Titel **Diverse Schwachstellen erlauben Remote Code Execution**	Risiko ■■■■■
Betroffene Systeme:	Google Chrome, <= 37.0.2062.94
Sachstand:	Über mehrere Schwachstellen in der Verarbeitung von Vektorgrafiken (SVG) sowie dem Objektmodell in HTML (DOM) kann ein Angreifer eigenen Code innerhalb sowie außerhalb der Sandbox seines Opfers zur Ausführung bringen.
Bewertung:	Mit dem Einschleusen fremden Codes in Zielsysteme kann ein Angreifer potenziell beliebige Aktionen im Kontext des angemeldeten Benutzers ausführen. Dies wirkt im vorliegenden Fall umso schwerer, als auch ein Verlassen der von Google Chrome eigentlich eingerichteten Sandbox möglich ist, wodurch Schadcode außerhalb des Browser-Tabs und somit system- bzw. netzwerkweit mit den Rechten des angemeldeten Benutzers ausgeführt werden kann. Updates auf nicht verwundbare Versionen sind bereits veröffentlicht.
Empfehlung:	1) Google Chrome sollte auf die Version 37.0.2062.94 oder neuer aktualisiert werden.
Quellen:	CVE-2014-3175 http://www.securitytracker.com/id/1030767 http://googlechromereleases.blogspot.de/2014/08/stable-channel-update_26.html
Point of Contact	Dominik Neubauer, dne@it-tuv.com, 0221/969789-82



2014-09-09: Information Disclosure im Internet Explorer

Titel **Information Disclosure im Internet Explorer**	Risiko ■■■□□
Betroffene Systeme:	Internet Explorer, Versionen 6 - 11, alle Windows-Betriebssysteme
Sachstand:	Die Zero-Day Schwachstelle ermöglicht einem Angreifer interne Informationen auszulesen, z.B. lokale Adresspfade, Netzwerkfreigaben, Rechnernamen und IP-Adressen von Systemen im internen Netz. Die Schwachstelle wurde bereits vermehrt in der Vergangenheit ausgenutzt.
Bewertung:	Durch Ausführung von schädlichem Code kann ein Angreifer unter Umständen sensible Informationen von Systemen auslesen und weitere Angriffe verfahren. Die Schwachstelle ist vergleichsweise einfach auszunutzen, da der Benutzer lediglich mit dem Internet Explorer auf eine manipulierte URL zugreifen muss.
Empfehlung:	1) Microsoft hat die Schwachstelle mit seinem August-Patchday geschlossen, die Updates sollten auf den Systemen der Benutzer installiert werden.
Quellen:	CVE-2013-7331 http://www.securityweek.com/microsoft-patches-internet-explorer-vulnerability-targeted-attackers https://technet.microsoft.com/library/security/ms14-sep
Point of Contact	André Zingsheim, azi@it-tuv.com, 0221/969789-83



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