

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	

