



RESPONSIVE DISCLOSURE POLICY

GERMAN

Wir gehen verantwortungsvoll mit Sicherheitsproblemen um. Dies betrifft Produkte die nicht durch Kunden der Rootsektor hergestellt wurden oder durch vertragliche Vereinbarungen von einer Veröffentlichung ausgeschlossen sind. Die Rootsektor hält sich an den eigens auferlegten Prozess der verantwortlichen Offenlegung von Sicherheitsschwachstellen welcher in der IT-Security Community allgemein anerkannt ist.

Produkthersteller werden in Form eines Security Advisory auf Schwachstellen vertraulich hingewiesen. Die Rootsektor steht bei Rückfragen zu den eigens erstellten Security Advisories beratend zur Verfügung.

Ein Security Advisory beinhaltet detaillierte Informationen zu der Schwachstelle mit welcher ein Hersteller die Schwachstelle nachvollziehen und untersuchen kann. Gemäß der Timeline unserer Policy werden Informationen veröffentlicht sobald der Hersteller einen Patch/Workaround erstellt hat oder nach 45 Tagen sollte seitens des Herstellers keine begründete Ausnahme bestehen, weshalb von der Veröffentlichung abgesehen werden soll. In oben genannten Ausnahmefällen kann zusammen mit dem Hersteller eine koordinierte Veröffentlichung stattfinden und ein alternativer Zeitplan erarbeitet werden.

Im Rahmen der Responsive Disclosure Policy wägen wir das Interesse der Öffentlichkeit über Sicherheitsprobleme zu Informieren gegenüber der effektiven Behebung durch den Hersteller ab.

Ziel ist es einen für beide Seiten vertretbaren Mittelweg zu finden.

ENGLISH

We are dealing with security issues in a responsible way. This affects products which are not produced by customers of Rootsektor or are excluded from public disclosure due to contractual agreements with vendors. The self imposed process of responsible disclosure is approved in the it security community.

Vendors get informed by a confidentially security advisory. Rootsektor provides assistant to the vendor for self released security advisories. A security advisory contains all details needed to reproduce and analyse the vulnerability in detail. According to our policy we will release information about the security vulnerability after the vendor fixed the problem or 45 days after we informed the vendor.

In well-founded exceptional cases, the date of disclosure can be adjusted with the vendor.

As part of the responsive disclosure policy we weigh up the public interest of the security vulnerability against the vendor's time to remedy all security issues effectively.

The goal of this responsive disclosure policy is, to weigh up both positions.