

SySS Responsible Disclosure Policy

Wir forschen und zeigen Verantwortung – Research and Responsibility

Die SySS GmbH geht verantwortungsvoll mit Sicherheitsproblemen um. Schwachstellen in Produkten, die nicht von Kunden der SySS GmbH hergestellt wurden oder allgemein durch vertragliche Vereinbarungen von einer Veröffentlichung ausgeschlossen sind, werden im Rahmen unseres Prozesses zur verantwortungsvollen Offenlegung von Sicherheitschwachstellen (Responsible Disclosure) schriftlich in Form eines Security Advisory an betroffene Hersteller gemeldet.

Das Security Advisory gibt detaillierte Informationen zu der gefundenen Schwachstelle, sodass der Hersteller das Sicherheitsproblem nachvollziehen und weiter untersuchen kann. Schwachstellen werden, nachdem der Hersteller eine Lösung bereitgestellt hat oder 45 Tage nachdem sie von der SySS GmbH vertraulich an den Hersteller gemeldet wurden, veröffentlicht. Das ist unabhängig davon, ob die Schwachstelle zu diesem Zeitpunkt durch einen Patch oder Workaround vom Hersteller behoben worden ist.

In begründeten Ausnahmefällen sind wir bereit von diesem Standardvorgehen abzuweichen und gemeinsam mit dem Hersteller einen alternativen Zeitplan für die koordinierte Veröffentlichung der Schwachstelle zu vereinbaren. Ziel der SySS Responsible Disclosure Policy ist es, überlegt das Interesse der Öffentlichkeit über Sicherheitsschwachstellen informiert zu sein gegen die Zeit für eine wirksame Behebung durch den Hersteller abzuwägen. Der endgültige Zeitplan für die Veröffentlichung einer Schwachstelle wird nach bestem Wissen unter Berücksichtigung dieser beiden Positionen gewählt. Die SySS GmbH bietet Herstellern die Möglichkeit, vor der Veröffentlichung einer Schwachstelle das Sicherheitsproblem zu analysieren, dieses zu beheben und durch ausführliche Tests die Lösung zu überprüfen.

SySS GmbH deals with security issues in a responsible way. In the form of a security advisory we report security vulnerabilities which are not in products of our customers and which are not excluded from public disclosure due to contractual agreements with vendors.

The security advisory contains detailed information about the found vulnerability that allows the vendor to reproduce and further investigate the reported security issue. Vulnerabilities will be disclosed to the public if a solution was published by the vendor or 45 days after the initial report by the SySS GmbH, regardless of the vulnerability status, for example if there is a patch or workaround from the affected vendor. In well-founded exceptional cases, this standard procedure may not be followed and an alternative, adjusted publication schedule will be negotiated with the vendor.

The goal of our Responsible Disclosure Policy is, to weigh up the need of the public to know of security vulnerabilities against the vendor's time to remedy all security issues effectively. The final publication schedule will be based on the best interests of the community overall, considering both positions. Before the responsible disclosure of a security vulnerability, the SySS GmbH allows vendors the opportunity to analyze reported security issues, to develop effective countermeasures, and to test them thoroughly.