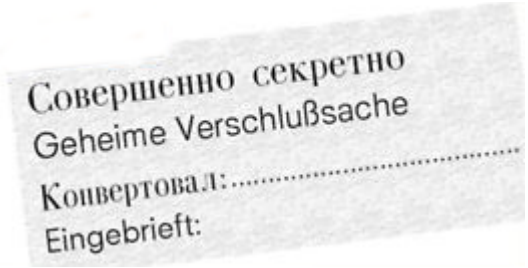

OXID PARTNERTAG 2017
09. NOVEMBER 2017, KONZERTHAUS FREIBURG

OXID
esales

OXID SECURITY PROZESS

OXID Security Prozess

- Was ist ein Security Issue?
- Wie kommen Security Issues zu uns?
- Wer ist das Security Team
- Next Steps

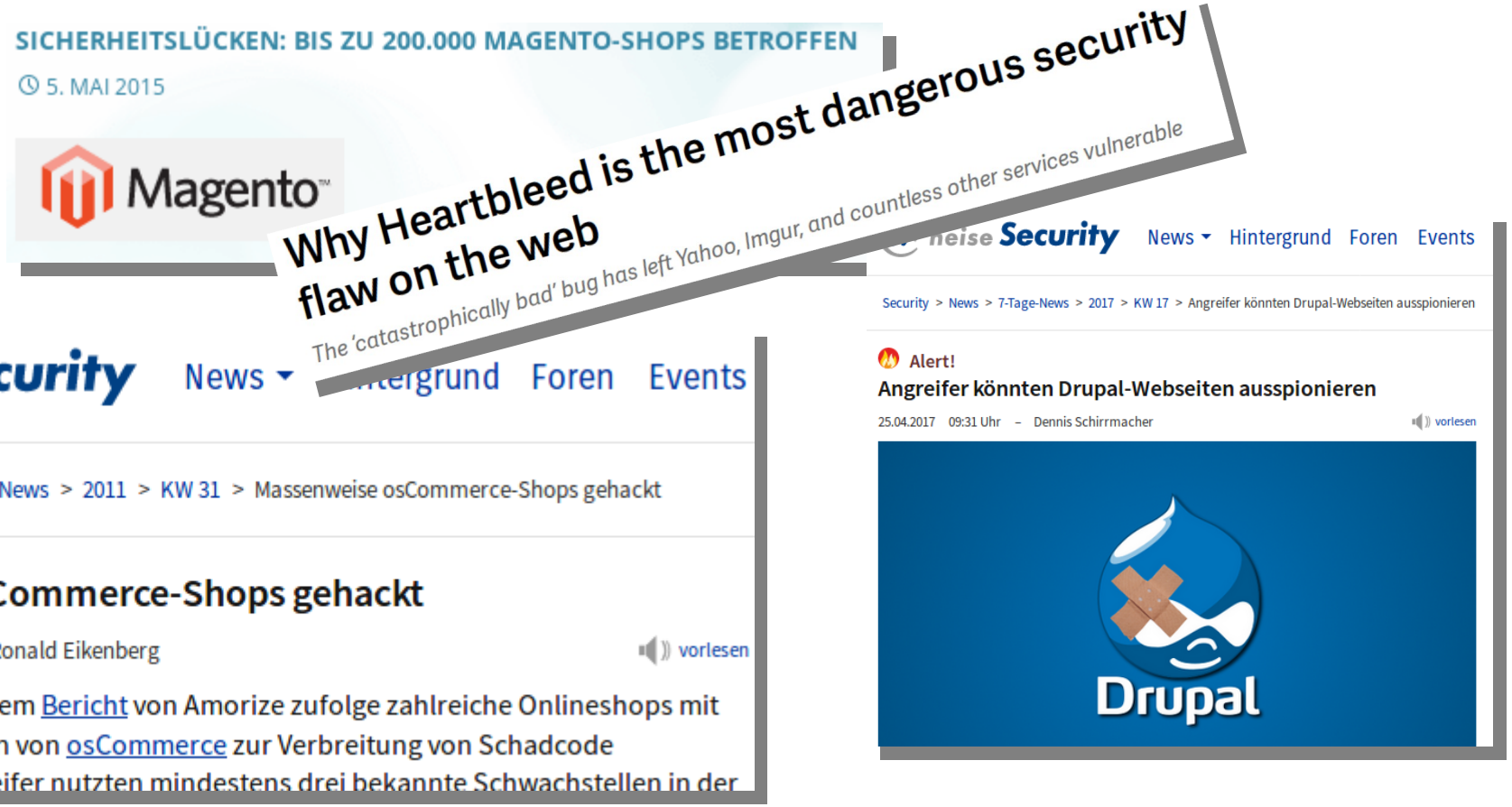


OXID esales

Was ist ein Security Issue?

- Eine Sicherheitslücke in OXID eShop, die von einem Angreifer ausgenutzt werden kann, um
  - Die fehlerfreie Ausführung der Applikation zu stören (z.B. DoS),
  - Unautorisiert Daten zu stehlen (z.B. „Scamming“),
  - Dem Händler finanziellen Schaden zuzufügen (z.B. sich selbst Vorteile beim Kauf verschaffen),
  - Sich unautorisiert Zugriff zur Applikation oder zum Server zu verschaffen, um z.B. Schadcode in die Applikation einzuschleusen (z.B. über XSS, Ausnutzung als Spamschleuder, Hosting für nicht erlaubte Inhalte etc.)

Warum ist das nicht nur für Händler kritisch?



Wie kommen Security Issues zu uns?

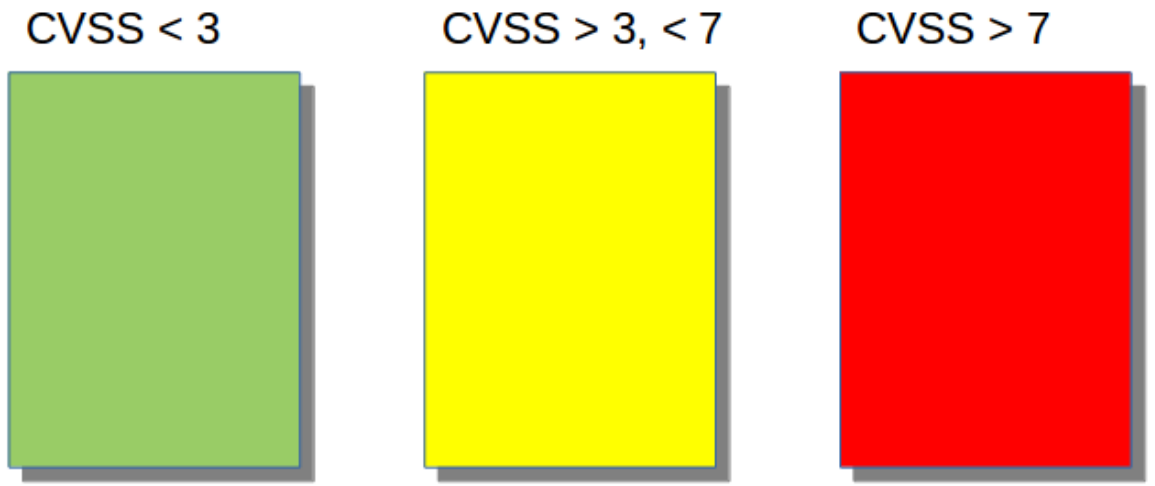
- https://oxidforge.org/en/security mit eindeutigen und klaren Anweisungen
- security@oxid-esales.com als Verteiler
- Bugtracker: Verweis auf security@ auf Startseite, wenn Security-Bug eingetragen wird, autom. E-Mail an security@
- Info@: Bitte beim kleinsten Verdacht an security@ weiterleiten
- Forum: Wird sofort mit Verweis auf security@ gelöscht
- Von:
  - Intern (Core- und PS-Team
  - Security Researcher (div. Unis, Beauftragte des TÜV, etc.)
  - Externe Entwickler, eher selten: Partner
  - „Lieschen Müller“

Wer ist das Security Team?

- E-Mails an security@ gehen an:
  - Security Team (ganz geheim ^^)
  - Core-Entwickler
  - Support
- Skalierbarkeit!
- Erfahrung im Umgang mit Security Issues

Next Steps

- Entwickler schätzen ein und versuchen zu Reproduzieren, informieren Security Team
- Antwort an Reporter
- CVSS „berechnen“
- Security Team erarbeitet Plan mit Deadlines zur Kommunikation



Next Steps: Code Green

- Wird als ganz normaler Security-Bug gefixt
- Erwähnung in den Release-Notes als „Security Improvement“
- Keine Vorab-Informationen
- Oft CSFR o.ä.
- Angreifer muss große Hürden nehmen, um kleinen Effekt zu erzielen

Next Steps: Code YELLOW

- Security Bulletin vorbereiten
- CVE Identifier beantragen bei MITRE
- Interne Information an Kollegen mit genauem Zeitplan, wer wann wie informiert wird
- Info an NDA-Owner, Partner, SLA-Kunden inkl. Security Bulletin und möglichst Workaround (Tutorial, Hotfix etc.)
- Release der gepatchten Version(en), inkl. Fix. Release Notes erhalten deutlichen Hinweis mit Bitte um schnellstmögliches Update.
- Ca. zehn Tage später Release des Security Bulletins
- Security Team trägt in div. Security-Datenbanken ein

Next Steps: Code RED

- Security Bulletin + FAQ vorbereiten
- CVE Identifier beantragen bei MITRE
- Interne Information an Kollegen mit genauem Zeitplan, wer wann wie informiert wird
- Info an NDA-Owner mit Security Bulletin
- Info an Partner, SLA-Kunden inkl. Security Bulletin und möglichst Workaround (Tutorial, Hotfix etc)
- Info Hosting Provider mit Rules für mod_security (SIWECOS-Projekt)
- Info BSI und Presse (SIWECOS-Projekt)
- Release der gepatchten Version(en), inkl. Fix. Release Notes erhalten deutlichen Hinweis mit Bitte um schnellstmögliches Update.
- Release des Security Bulletins am gleichen Tag wie OXID eShop Release
- Security Team trägt in div. Security-Datenbanken ein

Anmerkungen/Weiterführende Infos

- SIWECOS
- Unterstützte OXID eShop Versionen
  - Prinzipiell nur suportete Versionen (aktuell 5.3 und 5.2), ABER :-)
- Warum dieses Theater?
  - Professioneller Umgang, gute Wirkung nach Aussen
  - Besondere Herausforderung: Duale Lizenzierung
  - Vergleich mit / Abgrenzung zu anderen
- Whitepaper für den Vertrieb, ggf. weitere Vorträge, Blogpostserie, noch was (wie kann man Euch unterstützen)?
- Last not least: Marketingeffekt & kostenlose Security Audits ;)


OXID
esales