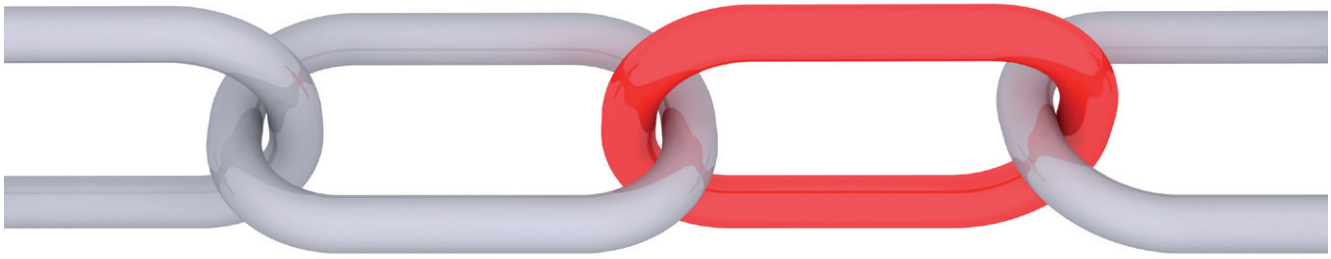
OXID
esales

Whitepaper

SICHERHEITSLÜCKE BEI OXID? UNSER PROZESS!

oxid-esales.com

INHALT



Als Hersteller von Software, die teils unter kommerzieller aber auch unter Open-Source-Lizenz distributiert wird, sind wir unseren Kunden und Benutzern gegenüber verpflichtet, sehr sorgsam mit gemeldeten Sicherheitslücken umzugehen.

Wir sind uns der Tatsache bewusst, dass insbesondere Shopsoftware eine geschäftskritische Anwendung sein kann und falscher Umgang, nicht vertrauliche Behandlung oder Informationen zum falschen Zeitpunkt zu einem finanziellen oder Imageschaden führen können. Deshalb bestehen wir darauf, den Kommunikationsprozess jederzeit selbst in der Hand zu halten.

1 EIN SECURITY ISSUE IN OXID ESHOP IST ...

eine Sicherheitslücke, die von einem Angreifer ausgenutzt werden kann, um

+ die fehlerfreie Ausführung der Applikation zu stören (z.B. DoS/Denial of Service),
+ unautorisiert Daten zu stehlen (z.B. „Scamming"),
+ dem Händler finanziellen Schaden zuzufügen (z.B. sich selbst Vorteile beim Kauf zu 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.).

2 WIE SOLCHE SICHERHEITSLÜCKEN ENTSTEHEN

Keine Software ist frei von Fehlern, so genannten „Software-Bugs"; dies gilt natürlich auch für sicherheitsrelevante Softwarefehler, die unabsichtlich entstehen. Auch die allerbeste Schulung zu hundertprozentig sicherer Programmierung wird menschlichen Aspekte wie „Übersehen", „Unaufmerksamkeit in diesem Moment" oder auch historische Fehler, an deren Ausnutzung noch vor Jahren niemand glauben konnte, nicht ausmerzen können. Insofern sind solche „Verfehlungen" in allen Systemen an der Tagesordnung.

Niemand gibt dies gern zu, weil es als Schwäche ausgelegt werden könnte. Gehen wir jedoch progressiv mit diesen Fehlern um, können wir größeren Schaden vermeiden. Dazu zwingen wir uns im Übrigen selbst, indem wir den Kern der Software als Open-Souce-Edition veröffentlichen und wissentlich in Kauf nehmen, dass diese auf Herz und Nieren von völlig Unbekannten überprüft werden kann und wird.

3 WAS AUF DEM SPIEL STEHT

Open-Source-Entwicklung ist öffentlich einsehbar, insofern könnten auch Sicherheitslücken direkt im Code ausgemacht werden. Das ist allein aufgrund der hohen Anzahl der LoC (Lines of Code) nicht einfach möglich, weshalb sich potentielle Angreifer auf Änderungen im Code, auf die sog. Commits, konzentrieren.

Besteht eine Sicherheitslücke, die – bevor Sie an den Hersteller gemeldet wird (also in diesem Fall an uns) – ausgenutzt wird, reden wir von einem sog. **„0-Day-Exploit“**, den wir innerhalb des OXID Universums bisher nur ein einziges Mal verzeichnen mussten.

Je nach Schwere der Angriffsmöglichkeit kann es durchaus passieren, dass die Reputation des Online-Händlers als auch die der Partneragentur oder der OXID eSales AG in Mitleidenschaft gezogen wird. Das kann im schlimmsten Fall zu einer ausgewachsenen PR-Krise lancieren, die einen enormen Imageschaden verursachen kann; das soll natürlich tunlichst vermieden werden.

4 SENSIBILISIERUNG

Korrekturen, die Sicherheitslücken beheben, stellen wir als Update zur Verfügung. Oft können auch Workarounds bereitgestellt werden, die (entsprechend angepasst) ggf. auch in nicht mehr unterstützten Versionen zum Einsatz kommen können. „Oft“ bedeutet eben „nicht immer“, sodass wir Kunden, Benutzer und Agenturen auf allen Kanälen dazu anhalten, möglichst nah am aktuellen Release zu arbeiten. Dazu müssen Updates und Upgrades von vorneherein geplant und insbesondere vom Shopbetreiber in das reguläre laufende Budget für die Softwaremaintenance mit einbezogen werden.

Sowohl Datenschützer (DSGVO) wie auch BSI (Bundesamt für Sicherheit im Internet) fordern Benutzer nicht ohne Grund auf, Software stets auf dem aktuellen Stand zu halten. Vermeintliche Argumente wie „dafür bin ich zu klein“, „wer soll denn mit meinen Daten etwas anfangen können“ sind Trugschlüsse!

5 WIE GELANGEN DIESE MELDUNGEN ZU UNS?

Wir unterziehen uns regelmäßig sowohl internen als auch von extern durchgeführten Sicherheitsaudits. Interessant ist, dass auch hier nicht immer alle potentiellen Schwächen sichtbar gemacht werden können. Potentielle Sicherheitslücken wurden in der Vergangenheit durch Entwickler, aber auch aus der Partner- und Kundenlandschaft, gemeldet. Zusätzlich erhalten wir Meldungen aus komplett externen Quellen wie z.B. von Sicherheitsbeauftragten in Kundenprojekten, Forschungsteams an Universitäten aus aller Welt, die scheinbar wahllos Open-Source-Projekte unter die Lupe nehmen.

Es gäbe nun verschiedene Möglichkeiten, solcherart Informationen in die Produktentwicklung einfließen zu lassen. Aber sowohl im Forum als auch im Bugtracker sind Moderatoren darauf konditioniert, diese Beiträge sofort zu schließen und uns die Informationen anderweitig zukommen zu lassen, damit diese noch vertraulich behandelt werden können. So werden z.B. Einträge in der Kategorie „Security“ im Bugtracker per E-Mail direkt an **security@oxid-esales.com** weitergeleitet.

6 SECURITY TEAM

Das Security-Team besteht aktuell aus drei Positionen:
Dem Entwicklungsleiter, einem Senior Technical Lead und einem Software Support Engineer. Die Zusammensetzung des Teams ist nicht zufällig gewählt und bietet verschiedene Vorteile: Der Prozess ist skalierbar und greift auch dann, wenn ein Mitglied des Teams nicht anwesend ist; dabei ist das Team nicht zu groß, um Entscheidungen schnell und unkompliziert treffen zu können. Ein weiterer, psychologisch nicht zu unterschätzender Aspekt: Die Verantwortung darf nicht alleine auf einem Schulterpaar liegen.

7 INTERNER AUFBAU DER ORGANISATION UND VERTEILUNG DER INFORMATIONEN

Die E-Mail-Adresse security@oxid-esales.com ist ein interner Verteiler. Folgende Gruppen werden benachrichtigt:

+ Das **Security-Team** antwortet umgehend auf eine eingesendete E-Mail mit der Information, dass wir uns schnellstmöglich darum kümmern, die potentielle Sicherheitslücke und die nachfolgenden Schritte einzuschätzen.
+ Das **Produktentwicklung-Team**, das sich umgehend mit der potentiellen Sicherheitslücke auseinandersetzt. Eine Einschätzung, ob es sich um eine reproduzierbare Sicherheitslücke handelt, welcher Schaden potentiell entstehen könnte und wie und mit welchem Aufwand der Fehler behoben werden kann, wird an das Security-Team zurückgemeldet.
+ Das **Support-Team**, um informiert zu sein und um ggf. unterstützend eingreifen zu können.

8 ERSTE EINSCHÄTZUNGEN

Nach Einschätzung durch die Entwickler kalkuliert das Security-Team den so genannten CVSS, einen Standard-Score mit einer Skala von 0 bis 10, an dem die Schwere der Sicherheitslücke eingeschätzt werden kann und berät über das weitere Vorgehen: Wann wird der Bug gefixt, wann wird wer informiert und wann wird die geschlossene Sicherheitslücke als Release herausgegeben. Dabei ist der CVSS ein wichtiger Indikator für diese Einschätzungen: Sich allein auf die menschliche Entscheidungskraft zu stützen, kann von verschiedenen Faktoren (Zeitmangel, Tagesform etc.) abhängig sein.

Je nach Schweregrad können nun drei verschiedene Prozesse angestoßen werden:

+ Ein CVSS < 3 = **Code:green**,
+ CVSS > 3 und < 7 = **Code:yellow** und
+ ein CVSS > 7 bedeutet **Code:red**.

Derjenige, der uns über die Sicherheitslücke berichtet hat, wird nun über die geplante Vorgehensweise informiert und zu Stillschweigen verpflichtet, bis das Release publiziert wurde.

9 VERSCHIEDENE PROZESSE NACH DEM AMPELPRINZIP

Auf Grundlage der CVSS-Einschätzung greifen verschiedene Prozesse, die hier im Einzelnen erläutert werden:

9.1 CODE:GREEN

Bei diesen Security Issues mit einem CVSS < 3 muss ein potentieller Angreifer sehr große Hürden nehmen, um einen relativ kleinen Schaden zu verursachen – mit anderen Worten, es lohnt sich einfach nicht. Oft handelt es sich um Angriffsmöglichkeiten, die z.B. als CSFR (Cross Site Forgery Request) klassifiziert werden.

+ Es wird keine CVE-Nummer (s.u.) beantragt.
+ Es wird kein Security Bulletin erstellt.
+ Der Bugtrack-Eintrag bleibt offen, Bug wird mit hoher Priorität bearbeitet, fließt in das nächste planmäßige Release mit ein.
+ Korrektur (Fix) erfolgt im offenen GitHub-Repository.
+ Es gibt keine interne Information der Mitarbeiter bei OXID.
+ Vorab-Informationen an Partner, Kunden und NDA-Owner werden nicht versendet.
+ In den Release-Notes wird unter Verweis auf den Bugtrack-Eintrag erwähnt, dass ein „Security Improvement" im Release enthalten ist.

9.2 CODE:YELLOW

Sicherheitslücken mit einem CVSS > 3 und kleiner als 7 werden mit dem Prozess ‚Code:yellow' bearbeitet. In einem typischen Angriffs-Szenario werden zum Beispiel fehlende Formular-Validierungen ausgenutzt; es ist etwas Mühe erforderlich und Schaden kann entstehen.

+ Eine CVE-Nummer wird bei MITRE beantragt.
+ Ein OXID Security Bulletin wird erstellt und auf der Online Dokumentation passwortgeschützt veröffentlicht.
+ Ein Bugtrack-Eintrag bleibt im Status „private", bis der Security Bulletin ohne Passwortschutz veröffentlicht wurde (ca. zehn Tage nach dem Release der neuen Version).
+ Korrektur erfolgt in einem geschlossenen GitHub-Repository, das kurz vor dem Release mit dem öffentlichen GitHub Repository zusammengeführt wird.
+ Alle Mitarbeiter mit Kundenkontakt erhalten einen genauen Zeitplan, wann Partner, Kunden und NDA-Unterzeichner informiert werden, wann das OXID eShop Release verfügbar ist und wann der Security Bulletin veröffentlicht wird.
+ Meist zehn bis 14 Tage vor dem Release ergeht eine Vorab-Nachricht an Partner, Kunden und NDA-Unterzeichner mit den Passwörtern für den Security Bulletin (der ggf. einen Workaround enthält) und einer Information über den Zeitplan der weiteren Schritte. In dieser Benachrichtigung bitten wir um Stillschweigen bis zum Release. Hält einer der Empfänger diese Regel nicht ein, wird er ab dem nächsten Empfang einer solchen Information gesperrt.
+ Es folgt das öffentliche Release der OXID eShop Suite, die einen Fix enthält. In den Release Notes findet sich ein deutlicher Hinweis auf behobene Sicherheitslücken und die Bitte um ein schnelles Update.
+ Ca. zehn Tage nach diesem Release wird der Security Bulletin veröffentlicht wie auch die Bugeinträge in den Status „public" versetzt (sofern auch die Community Edition betroffen ist).
+ Neben MITRE wird auch an verschiedene andere Security-Datenbanken gemeldet.

9.3 CODE:RED

Bei einem Code:red handelt es sich um eine Sicherheitslücke mit einem kalkulierten CVSS > 7. Als Beispiel seien hier genannt: Komplett von außen offene Zugriffe auf die API oder auch die Möglichkeit, sich über das Frontend des Shops Admin-Zugriff zu verschaffen. Hierbei ist der Aufwand für einen Angriff oft gering. Es kann maximaler Schaden entstehen. Deshalb basiert der Prozess im Wesentlichen auf den gleichen Schritten wie im Abschnitt „Code:yellow" beschrieben, differenziert sich aber durch folgende Vorgehensweisen:

+ Wir behalten uns in diesem Fall vor, ein OXID eShop Release außerhalb der üblichen Release-Zyklen (vierteljährlich) zu veröffentlichen.
+ Zusätzlich zu einem Security Bulletin wird eine FAQ auf der Online Dokumentation erstellt, die spätestens ab der Veröffentlichung des Security Bulletins öffentlich zugänglich ist. Diese FAQ ist vorrangig an eine Leserschaft gerichtet, die des Lesens von Security Bulletins nicht mächtig ist und dient als „Landingpage" für weitere Veröffentlichungen (s.u.)
+ Die o.g. Vorab-Benachrichtigung von NDA-Unterzeichnern, Partnern und Kunden wird zeitlich gesplittet: Zunächst werden NDA-Unterzeichner informiert, wenige Tage später Partneragenturen und Kunden ohne NDA. Diese Vorgehensweise soll sicherstellen, dass Partner über diese Vorgänge und Zeitpläne informiert sind, bevor sie ggf. ahnungslos von ihren Kunden mit der Tatsache konfrontiert werden.
+ Wir stellen für Hosting Provider (nicht nur Hosting Partner!) Regeln für das Apache-Modul mod_security zur Verfügung. Eine Mailingliste dafür erhalten wir über die Zusammenarbeit mit dem SIWECOS-Projekt, dem CMS-Garden und befreundeten Open Source CMS- und Shopsystemen. Diese Regeln dienen dazu, dass der Hosting Provider als Server-Inhaber in die Lage versetzt wird, entsprechende Anfragen an den Webserver direkt ins Nirvana zu leiten und sich so des Supportaufwandes im Angriffsfall zu entledigen.
+ Wir informieren sowohl das BSI (Bundesamt für Sicherheit im Internet) wie auch Fachpresse (z.B. heise.de, golem.de usw.), um eine möglichst große Empfängergruppe und insbesondere Benutzer des OXID eShop zu erreichen und zum Update zu bewegen.
+ Im Unterschied zur Vorgehensweise bei Code:yellow wird der Security Bulletin wie auch der Eintrag im Bugtracker gleichzeitig mit dem Release einer neuen OXID eShop Version veröffentlicht, da ggf. nur Stunden bis zum ersten Angriff vergehen könnten.

10 MODULE UND ERWEITERUNGEN

In der OXID eShop Suite ausgelieferte Module und Erweiterungen werden über die o.g. Prozesse einbezogen. Wir halten engen Kontakt zu den Herstellern dieser Module, um reibungslosen Informationsfluss und Integration in die Suite zu gewährleisten.

Module, die nicht mit der OXID eShop Suite ausgeliefert werden, können nicht über diesen Prozess behandelt werden. Hier empfiehlt sich der direkte Kontakt zum Hersteller.

11 ÜBER SICHERHEITSLÜCKEN AUF DEM LAUFENDEN BLEIBEN

Es gibt verschiedene Möglichkeiten, sich über Sicherheitslücken informieren zu lassen:

+ Partner, Kunden und NDA-Unterzeichner werden vorab per E-Mail informiert (s.o.)
+ Neue Releases werden über Release-Notes veröffentlicht, enthalten die Information, dass Sicherheitslücken behoben wurden (Code:yellow und Code:red).

12 DOKUMENTATION BISHERIGER SICHERHEITSLÜCKEN

Bisherige Security Bulletins werden hier abgelegt: **https://security.oxid-esales.com/security-bulletins**.

13 NACHARBEITEN

Nach jedem abgeschlossenen Fall setzt sich das Security-Team noch einmal zu Nacharbeiten zusammen und berät darüber, was gut und was schlecht gelaufen ist, wo es evtl. Nachbesserungen im Prozess geben muss oder welche Entscheidungen an anderer Stelle im Unternehmen zu treffen sind. Dazu befragen wir häufig Partner und Kunden und erhalten so wertvolles Feedback, das wir für den nächsten Fall übernehmen können.

KONTAKT

Für Fragen zum Security Prozess oder Anmerkungen wenden Sie sich bitte gern direkt in englischer Sprache an das Security Team unter **security@oxid-esales.com** oder besuchen Sie **https://security.oxid-esales.com.**

OXID eSales AG
Bertoldstraße 48
79098 Freiburg, Germany

Tel. +49 761 368 89 0
Fax +49 761 368 89 29
info@oxid-esales.com

www.oxid-esales.com
www.twitter.com/OXID_eSales
www.facebook.com/OXID.eSales