DGI-2 Security

Richtlinie zur Meldung und Bearbeitung von Sicherheitsproblemen bei Software im D-Grid

Version 1.0, 14.02.2012

D-Grid Integrationsprojekt 2 (DGI-2)

Autoren

Benjamin Henne, Christian Szongott, Christopher Kunz (RRZN, Leibniz Universität Hannover)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IG07014F gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Versionsgeschichte

Revision	Datum	Bearbeiter	Anmerkungen
0.1	10.11.2011	C. Kunz / RRZN	Framework
0.2	01.12.2011	C. Szongott	Textuelle Erweiterungen
0.3	05.12.2011	B. Henne	Überarbeitung, Einbettung D-Grid Betriebskonzept
0.4	19.01.2012	C. Szongott	Überarbeitung, Einarbeitung Feedback
1.0	14.02.2012	C. Szongott / B. Henne	Überarbeitung und Finalisierung

Inhalt

1 Einführung

Das D-Grid ist wie jede andere verteilte Infrastruktur stetigen Angriffen ausgesetzt. Diese Angriffe richten sich häufig gegen die im D-Grid eingesetzte Software und dabei speziell gegen die Komponenten der verwendeten Middleware, welche auf allen Ressourcen der D-Grid-Infrastruktur installiert sind. Schwachstellen in der verwendeten Software werden nicht nur von potentiellen Angreifern entdeckt, sondern auch durch Sicherheitsforscher oder durch Teilnehmer des D-Grids.

Aufbauend auf dem D-Grid Betriebskonzept (Version 2.0 vom 04.12.2009) liefert dieses Dokument einige Handreichungen für die Meldung und die Behandlung sicherheitsrelevanter Probleme für die im D-Grid eingesetzte Software. Es listet zudem relevante Informationsquellen für Grid-Nutzer und Grid-Site-Betreiber auf, welche sich mit Software-Security befassen.

2 Begriffsdefinitionen

2.1 Relevante Software

Auf den Ressourcen der D-Grid-Sites wird gemäß der DGI-Referenzinstallation 2011.2 [DGI-Ref] derzeit folgende Software eingesetzt:

- Scientific Linux 4.x und 5.x
- Globus Toolkit 4.0.8, 4.2.1, 5.0.x
- gsissh
- OGSA-DAI 2
- UNICORE 6.4
- gLite CREAM 3.2
- dCache 1.9.5
- JavaGAT 2
- cfengine 3
- Batch-Systeme Torque, Sun-Grid-Engine
- Clients für D-Mon und D-Grid-Accounting
- dgridmap

Der Statusbericht über die Kern-Grid-Infrastruktur (01/2011)[1] [D-Grid-Status] zeigt, dass auch ältere Versionen und weitere Software an den Sites installiert sind:

- gLite 3.1
- dCache 1.8
- UNICORE 6.x
- Storage-Resource-Broker (SRB)
- iRods

Darüber hinaus wird projekteigene Software der Communities/VOs eingesetzt.

Auf den zentralen Komponenten der der Kern-Infrastruktur wird folgende Software betrieben:

- VOMS
- VOMRS
- GRRS
- D-Mon
- DGAS-Accounting
- Nagios-Monitoring

2.2 Was ist ein Sicherheitsproblem in Software?

Eine Sicherheitslücke liegt vor, wenn eine Person Zugriff über die ihr zustehenden Rechte hinaus auf ein gegen Zugriff besonders geschütztes System erlangt. Das beinhaltet den unberechtigten Zugriff durch Dritte, denen keine Zugriffsrechte eingeräumt wurden, aber auch die unbeabsichtigte Erhöhung der Privilegien, die einem legitimen Nutzer eingeräumt werden. Darüber hinaus liegt eine Sicherheitslücke vor, wenn durch eine Aktion das System beschädigt oder zerstört werden kann. Zusammengefasst all die Fälle, in denen die Integrität, die Vertraulichkeit oder die Verfügbarkeit eines Systems durch Dritte beeinträchtigt wird.

[1] http://d-grid-ggmbh.de/fileadmin/downloads/Berichte/Statusbericht_Kern0111.pdf

Ein wichtiges Kriterium für die Klassifikation eines Softwarefehlers als Sicherheitslücke ist die Möglichkeit, diese Lücke reproduzierbar auszunutzen. Hierfür ist ein “Proof of Concept”-Exploit hilfreich.

2.3 Welche Sicherheitsprobleme sind nicht relevant?

Nicht relevant für die Betrachtung im vorliegenden Dokument sind folgende Sicherheitslücken:
Lücken, für deren Ausnutzung administrativer Zugriff notwendig ist (etwa Fehler in einem webbasierten Admin-Backend). Administratoren von D-Grid-Ressourcen werden als vertrauenswürdige Personen behandelt und werden auf ihren Ressourcen und auf den gemeinsam genutzten Ressourcen im D-Grid privilegiert behandelt.
Lücken, die lediglich Informationen für einen weiteren Angriff liefern (“Information Disclosure”) können je nach Schwere entweder als Lücken der niedrigsten Stufe oder als nicht sicherheitsrelevante Software-Bugs behandelt werden.

2.4 Skala für die Einstufung von Sicherheitsproblemen

Die folgende Skala soll einen Anhaltspunkt für die Wichtigkeit einer Sicherheitslücke liefern. Sie enthält im Feld “Beschreibung” jeweils einige typische Indizien, von denen nur eines gegeben sein muss.

Stufe	Beschreibung
Kritisch	- Sicherheitslücke ermöglicht Übernahme des Systems oder eines Teilsystems durch unbefugte Dritte - Anwendung wird durch Ausnutzung der Sicherheitslücke für alle Nutzer unbenutzbar (Denial of Service) - Sicherheitslücke ermöglicht Ausführung beliebigen Schadcodes durch Angreifer - Lücke ist immer und leicht ausnutzbar
Hoch	- Sicherheitslücke ermöglicht authentifizierten Nutzern eine Privilegien-Erhöhung - Sicherheitslücke ermöglicht Ausführung von Code durch Angreifer nur in einem begrenzten Kontext (z.B. nichtpersistenter XSS) - Anwendung wird durch Ausnutzung der Sicherheitslücke für einige Nutzer unbenutzbar - Ausnutzung der Lücke ist mit einigem Aufwand und nicht immer möglich
Mittel	- Sicherheitslücke erleichtert die Überwindung von Sicherheitsmechanismen (z.B. schwache Verschlüsselung) - Ausnutzung der Lücke ist nur schwierig und selten möglich
Niedrig	- Information Disclosure - Ausnutzung der Lücke nur unter vielen Randbedingungen möglich

3 Bearbeitung von Sicherheitsproblemen in Software

Findet ein D-Grid-Anwender oder ein Site-Administrator eine gemäß Abs. 2.2 relevante Sicherheitslücke in einer im D-Grid eingesetzten Software, so tritt der folgende Arbeitsablauf in Kraft:

3.1 Empfänger für gemeldete Sicherheitsprobleme

Sicherheitsprobleme sollten stets an die Mailadresse NGI-DE-CSIRT@LISTSERV.DFN.DE gemeldet werden. Diese Funktionsadresse ist ein Verteiler an die CERTs von KIT und DFN, so dass die im D-Grid-Kontext relevanten Stellen in jedem Fall informiert werden.

Ebenso besteht eine Hotline des DFN-CERTs (+49 40 808077 590), die Administratoren auch bei Grid-spezifischen Sicherheitsfragen und Problemen beratend zur Seite steht.

3.2 Inhalt einer Problemmeldung

Die Problemmeldung sollte mindestens folgende Informationen enthalten:
- Genaue Versionsbezeichnung der betroffenen Software
- Systemumgebung (Betriebssystemart und -version)
- Schritte, die zur Entdeckung der Sicherheitslücke geführt haben
- Wenn möglich, Anleitung zur Reproduktion der Sicherheitslücke („Proof of Concept“-Exploit)
- Eigene Einschätzung der Gefährlichkeit anhand der in Abs. 2.4 aufgeführten Skala
- Kontaktinformationen des Meldenden

3.3 Recherche und Weitermeldung

Sobald eine Meldung über die Funktionsadresse NGI-DE-CSIRT@LISTSERV.DFN.DE erfolgt ist, wird die Bearbeitung von den beteiligten CERTs übernommen. Diese ermitteln zunächst die zuständigen Entwickler und melden die gefundene Sicherheitslücke an diese weiter.
Die Validierung der Sicherheitslücke in einer Testumgebung gehört nicht zu den Aufgaben des CERT.

3.4 Behebung der Lücke

Der Softwarehersteller wird vom CERT mit der Meldung einer Lücke zu deren Behebung aufgefordert. Diese sollte abhängig von der Gefährlichkeit des gemeldeten Problems in folgendem Zeitrahmen erfolgen:

- Kritisch - 3 Tage
- Hoch - 6 Wochen
- Mittel - 4 Monate
- Niedrig - 1 Jahr

3.5 Ausgabe eines Security Advisories

Nach Behebung des Problems wird - koordiniert durch die CERTs in Absprache mit dem Softwarehersteller - ein Security Advisory verfasst und auf dem DFN-Portal veröffentlicht. Sollte ein Softwarehersteller nicht gewillt oder in der Lage sein, das Problem zu beheben, oder sollte sich das Problem nicht ohne Weiteres lösen lassen, so wird ein entsprechender Workaround erarbeitet und veröffentlicht.

4 Informationsquellen für D-Grid Teilnehmer

4.1 Einheitliche Ansprechpartner

Wie im Betriebskonzept des D-Grid festgeschrieben muss jede Grid-Site eine Kontakt-Emailadresse der Form dgrid-security@<site> betreiben. Diese dient zur Kontaktaufnahme bei Sicherheitsvorfällen und kann ebenso zum Abonnement von Advisories verwendet werden. Es wird empfohlen, dass unter der Kontakt-Emailadresse nicht nur eine einzelne Person erreichbar ist. Stattdessen ist die Weiterleitung an eine Mailingliste (wie oft auch bei abuse@domain.tld) mit einer möglichst großen Leserschaft ratsam.

4.2 Kommunikation von Software-Schwachstellen

Sicherheitshinweise werden vom DFN-CERT unter der URL https://portal.cert.dfn.de/adv/ öffentlich publiziert. Jeder Besitzer eines gültiges DFN- oder GridKa-Zertifikates kann dort zudem ein persönliches Email-Abonnement dieser Informationen konfigurieren.

Wichtige Sicherheitsinformationen können innerhalb des DFN-CERT Portals abonniert werden. Alle relevanten Sicherheitsinformationen können auf diese Weise automatisch an Interessierte weitergeleitet werden. Administratoren von D-Grid Sites sind angehalten, ein solches Abonnement einzurichten.

5 Anforderungen an Software-Hersteller im D-Grid

5.1 Einheitliche Ansprechpartner

Jeder Hersteller von Software soll einen einheitlichen Ansprechpartner für Sicherheitsfragen stellen. Dieser Ansprechpartner (Funktionsadresse) soll in der Dokumentation der Software benannt sein und an die zentrale Funktionsadresse für Security-Fragen des D-Grid (s.o.) gemeldet werden. Zudem sollte jeder Hersteller das D-Grid darüber in Kenntnis setzen, wo (Webseite, RSS-Feed o.ä.) aktuelle Sicherheitsinformationen zu seinen Produkten abrufbar sind.

5.2 Standardformat für Meldungen

Sofern ein Hersteller selbständig Sicherheitslücken gefunden und behoben hat, so sollte ein entsprechendes Security Advisory auf der in Abs. 5.1 genannten Informationsquelle veröffentlicht werden. Zusätzlich zu der allgemein lesbaren Version dieses Advisories sollte eine maschinenlesbare Version vorgehalten werden. Idealerweise soll diese Version im „Deutschen Advisory Format“, wie es vom Zusammenschluss der deutschen CERTs entwickelt wurde, vorliegen. Eine Formatbeschreibung dieses XML-basierten Formats ist unter http://www.cert-verbund.de/daf/daf_description.html abrufbar.

5.3 Versionsinformationen

Software wird oft in verschiedenen Versionen vom Hersteller angeboten und vom Anwender benutzt. Ein Beispiel für diese Versionierung ist das Globus Toolkit, das derzeit (Ende 2011) im D-Grid in 3 verschiedenen Versionen zur Anwendung kommt. Zur Identifikation relevanter Lücken ist es hilfreich, wenn der Hersteller Informationen über die Aktualität seiner Software bereitstellt. Insbesondere sollten durch diese Informationen folgende Fragen beantwortet werden:

- Welcher Versionszweig gilt als aktuell („Stable“, „Release“)?
- Welche älteren Versionen sind noch nennenswert verbreitet und werden weiter mit Sicherheit-supdates versorgt („Old Stable“)?
- Welche veralteten Versionen werden nicht mehr gepflegt („End of Life“)?

6 Referenzen

[DGI-Ref] D-Grid Referenz-Installation. Online: http://http://dgiref.d-grid.de/

[D-Grid-Status] Statusbericht über die Kern-Grid-Infrastruktur 01/2011.
Online: http://www.d-grid-gmbh.de/index.php?id=115