Dienste des DFN-CERT für die Grid-Communities

D-Grid Security Workshop

29.-30. 9. 2010, Göttingen

Gerti Foest, DFN

Aufgaben DFN-CERT

DFN-CERT unterstützt die Anwender bei Sicherheitsfragen

- Proaktiv (z.B. Info zu neuen Schwachstellen)
- Reaktiv (Unterstützung bei Vorfällen)
- Aus- und Fortbildung (Workshops, Tutorien)
- Nationale und internationale Kooperation (FIRST, TF-CSIRT, CERT-Verbund)

Unterstützung der Grid-Community

- Zusammenarbeit DFN-CERT <-> KIT-CERT

- 2 tägiges Treffen KIT-CERT/DFN/DFN-CERT im April 2010 in Hamburg
  - Wer macht was im Grid-Bereich – national/international?
  - Wo sind die Unterschiede, wo die Gemeinsamkeiten?
  - Wer nutzt welche Informationskanäle?
  - Wie können wir gemeinsam die Grid-Community noch besser unterstützen?

- Ergebnisse (u.a.):
  - Bekanntmachen in der Grid-Community, z.B. durch Vorträge auf diesem Security Workshop
  - Gegenseitige Aufnahme in relevante Mailinglisten

Woher bekommt man Informationen?

Am 20.09.2010 15:51, schrieb Buehler, Wilhelm:

Hallo Frau Foest, hallo Herr Pattloch,

> in der D-Grid-TAB-Sitzung heute (http://www.d-grid.de/tab/) wurde über den aktuellen Linux-Kernel-Exploit gesprochen. Es war den Teilnehmern nicht klar, wie diese Informationen im D-Grid "nach Plan" verteilt werden.
>
> Eine Idee aus dem TAB ist, diese Informationen auf jeden Fall auch an die Ressourcenprovider-Liste des D-Grids, die wird automatisch gefüllt und sollte aktuell sein.

Mit freundlichen Grüßen

Wilhelm Bühler

Aus dem DFN-CERT Portal

DFN-CERT Portal
Schwachstellen

Willkommen | Schwachstellen | Hilfe

Übersicht | Archiv | Konfiguration | Informationen

Hier können Sie das Archiv der bisher vom DFN-CERT verschickten Informationen über Schwachstellen durchsuchen.

[ ] Grid Suchen

Ihre Suchergebnisse (3 Treffer):

Datum	Titel	Systeme
17.09.2010	DFN-CERT-2010-1228: Kritische Kernelschwachstelle im Linux Kernel	Linux, Debian, Fedora, Mandriva, RedHat, SuSE, Grid
07.01.2010	DFN-CERT-2010-0018: Schwachstelle in Condor vor Version 7.4.1	Linux, Fedora, Grid
22.12.2009	DFN-CERT-2009-1812: Schwachstelle in Condor vor Version 7.4.1	Linux, RedHat, Grid

Meldung zur Schwachstelle im Linux Kernel (1)

DFN-CERT-2010-1228: Kritische Kernelschwachstelle im Linux Kernel

Historie

Version 1.0 (2010-09-17 11:40) Neues Advisory

Betroffene Software

Kernel

Betroffene Plattformen

Alle Linux Distributionen, welche einen Kernel der Versionen 2.4 und 2.6 einsetzen auf der x86_64 Architektur einsetzen und die Ausführung von 32-Bit Binaries ermöglichen.

Lösung

Workaround

Um die Auswirkungen der Schwachstelle einzuschränken, kann die Ausführung von 32-Bit Executables auf einem betroffenen System verhindert werden.

http://seclists.org/fulldisclosure/2010/Sep/273

Patch

Patch welcher die Schwachstelle CVE-2010-3081 behebt.

http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=c41d68a513c71e35a14f66d7

Patch

Patch welcher die Schwachstelle CVE-2007-4573/CVE-2010-3301 behebt.

http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=36d001c70d8a0144ac1d

http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=eefdca043e8391dcd719

Beschreibung

Zwei im Linux Kernel enthaltene Schwachstellen die bei der Ausführung von 32-Bit Binaries auf Systemen mit 64-Bit Architektur auftreten, erlauben es einem lokalen Angreifer Administratorrechte auf einem betroffenen System zu erlangen. Exploits sind für die Schwachstellen veröffentlicht.

Meldung zur Schwachstelle im Linux Kernel (2)

Schwachstellen

CVE-2010-3081: Schwachstelle im Linux Kernel der x86_64 Architektur

Im Linux Kernel für die x86_64 Architektur wird bei der Emulation eines IA32 der Wert des Stack-Pointers falsch in einen 64-Bit Wert konvertiert. Dabei kann es zu einem Underflow des Stackpointers kommen was dazu führt, dass dieser in den Speicherbereich des Kernels zeigt. Da keine Überprüfung des Wertes des Stackpointers durchgeführt wird, bleibt der Fehler unbemerkt und erlaubt es einem lokalen Angreifer Daten in den Speicherbereich des Kernels zu schreiben und mit dessen Rechten auszuführen.

Bitte beachten Sie, dass bereits ein Exploit für diese Schwachstelle veröffentlicht wurde.

CVE-2007-4573, CVE-2010-3301: Schwachstelle im Linux Kernel der x86_64 Architektur vor Version 2.6.22.7

Im Linux Kernel vor Version 2.6.22.7 für die x86_64 Architektur wird bei der Emulation eines IA32 Systemaufrufs die Nummer des Systemaufrufs im Akkumulator übergeben.
Durch die Emulation wird nur auf 32 Bit des Registers zugegriffen. Beim Ausführen des Systemaufrufs ptrace() werden die restlichen 32 Bit nicht initialisiert, so daß ein dort bereits vorhandener Wert für die Berechnung der anzuspringenden Funktion mit berücksichtigt wird. Ein lokaler Angreifer kann durch entsprechende Vorbelegung des gesamten 64 Bit Registers evtl. Befehle mit den Rechten des Kernels ausführen oder das System zum Absturz bringen.

Bitte beachten Sie, dass mehrere Exploits zu dieser Schwachstelle veröffentlicht sind.

Referenzen

Das Hersteller Advisory https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2010-3081

Schwachstelle CVE-2007-4573 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4573

Schwachstelle CVE-2010-3301 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3301

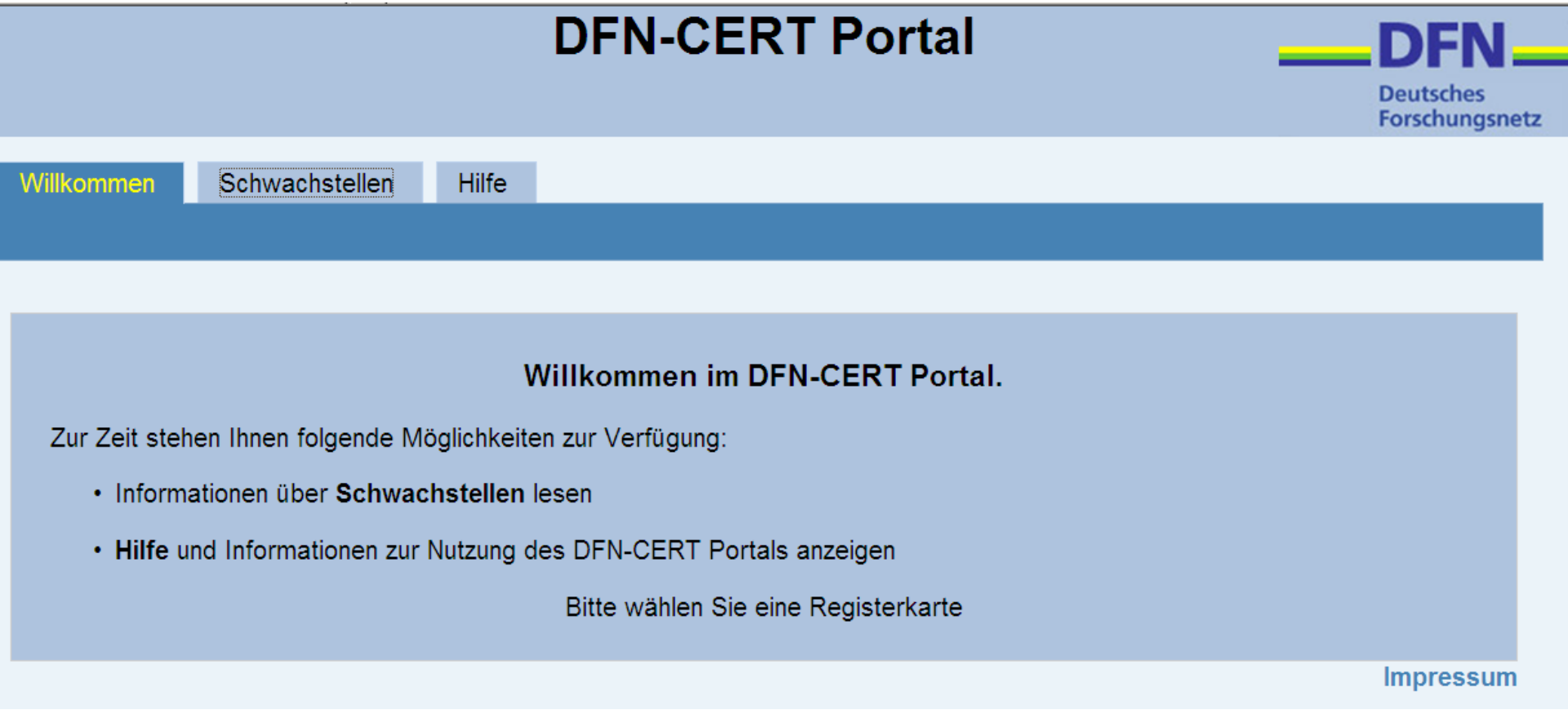
Schwachstelle CVE-2010-3081 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3081

Die Originalbeschreibung der Schwachstelle von Ben Hawkes http://sota.gen.nz/compat1/

Das DFN-CERT Portal

https://portal.cert.dfn.de

Zugriff ohne Zertifikat



Zugriff mit freigeschaltetem Zertifikat

1. Information zu Schwachstellen (proaktiv)

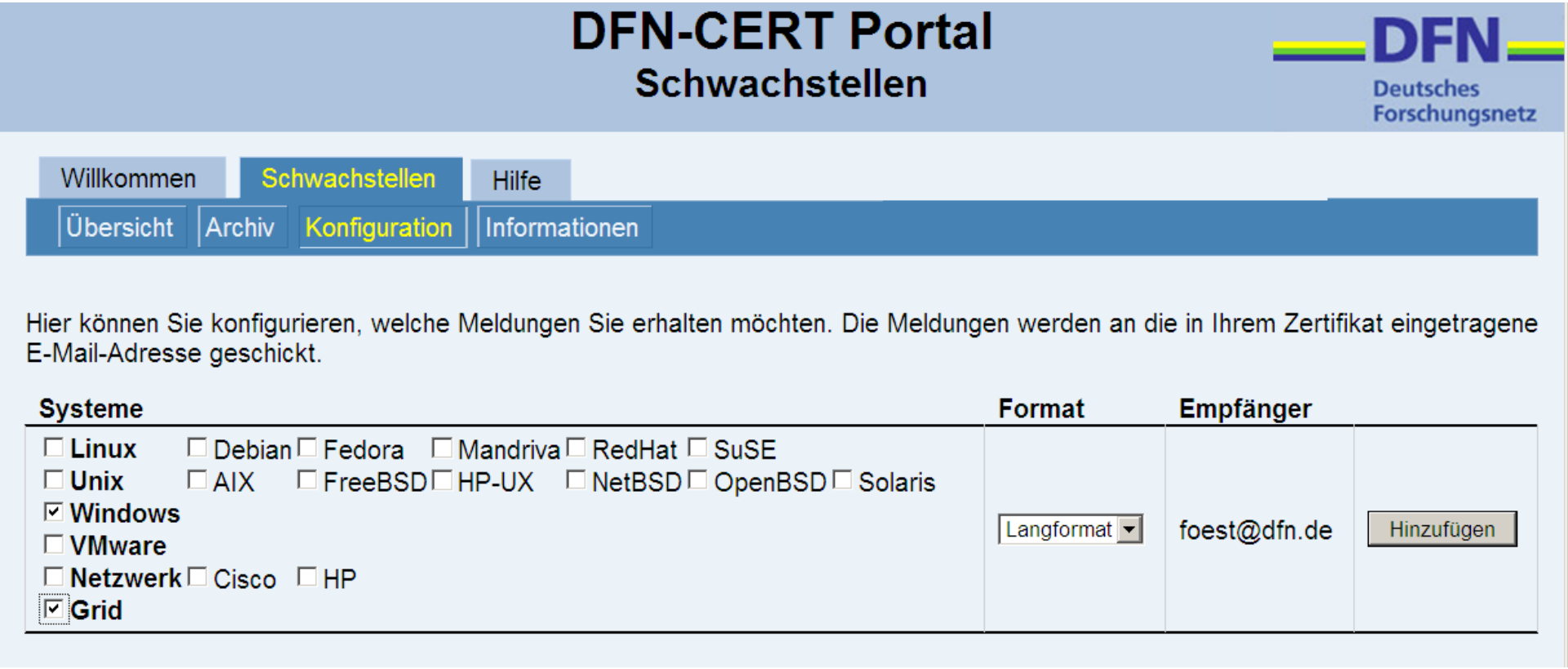
Informationen über Schwachstellen

- Verteilung bisher über die Mailingliste win-sec-ssc@lists.dfn-cert.de

- Schwachstellen-Archiv:
  - Alle versendeten Meldungen befinden sich im Archiv
  - Zugriff auf das Archiv ist für jedermann möglich (ohne Zertifikat)
  - Suchmöglichkeiten nach Kategorien, Meldungsnummern etc.

- Schwachstellen-Abonnement
  - Mit einem Zertifikat der DFN-PKI Global kann ein Abonnement (z. B. nur Grid-Systeme) konfiguriert werden

Konfiguration Schwachstellen



2. Warnmeldungen zu Vorfällen (reaktiv)

Automatische Warnmeldungen

- Konfigurierbare Meldungen zur regelmäßigen Information der Einrichtungen über Auffälligkeiten in ihren Netzbereichen
- Einbindung verschiedener Datenquellen
- Derzeit über 220 teilnehmende Einrichtungen
  - mehr als 98 % der IP-Adressen im X-WiN
- Zugriff nur für “handlungsberechtigte Personen” mit
  - Zertifikat der DFN-PKI Global
  - Schriftlicher Ernennung durch die Anwender-Einrichtung

DFN-CERT Portal
Automatische Warnmeldungen

DFN Deutsches Forschungsnetz

Willkommen | Schwachstellen | Automatische Warnmeldungen | Hilfe

Übersicht | Konfiguration | Informationen

Name Ihrer Einrichtung: HS Musterstadt

Netzbereiche verstecken

Folgende Netzbereiche sind nach Informationen des DFN-Vereins Ihrer Einrichtung zugeordnet:

Netzbereich	Erste Adresse	Letzte Adresse
172.16.0.0/16	172.16.0.0	172.16.255.255
172.31.12.0/23	172.31.12.0	172.31.13.255
172.31.17.0/25	172.31.17.0	172.31.17.127

Falls diese Angaben nicht zutreffend oder unvollständig sind, schicken Sie bitte eine E-Mail an cert@dfn.de.

Neue Regel einfügen

Die Regeln werden in der angegeben Reihenfolge von oben nach unten bearbeitet. Nur die erste passende Regel wird angewendet.

	Aktiv?	Netzbereiche	Intervall	Leermeldungen?	Empfänger	Betreff	
	Ja	Alle	Mo - Fr	Nein	security@hs-musterstadt.de	AW	Ändern

Regel für diese IP finden

Regeln exportieren | Regeln importieren

Beispielmeldung

Deutsches Forschungsnetz

```
Liebe Kolleginnen und Kollegen,
dies ist eine automatische Warnmeldung des DFN-CERT. In
den letzten Tagen erhielten wir Informationen über mög-
liche Sicherheitsprobleme auf Systemen in ihrem Netzwerk.
Netzblock: xxx.xxx.0.0/16
Kontakte: aw-dienst@example.com
Meldungen:
IP                Meldungstyp     Zuletzt gesehen
-------------------------------------------------------
xxx.xxx.181.16    Bot             2009-09-24 21:22:06
xxx.xxx.117.155   Virus/Wurm      2009-09-24 02:16:00
xxx.xxx.230.149   Spam Beschwerde 2009-09-24 02:27:35
...
```

Statistik - Vorfälle

- Mehr als 300 kompromittierte Rechner pro Tag
  - ca. 7.000 pro Monat
  - insgesamt bisher: knapp 100.000

- Hauptprobleme
  - Conficker
  - übernommene Rechner sind Teil eines Botnets
  - übernommene Rechner versenden Spam

3. Netzwerkprüfer (proaktiv)

Netzwerkprüfer

- Scan der Netzbereiche einer Einrichtung von außen
- Scans können vom Anwender konfiguriert und gestartet werden
- Darstellung der Ergebnisse im DFN-CERT Portal
- Periodische Scans zeigen (gewünschte / ungewünschte) Änderungen
- Zugriff nur für “handlungsberechtigte Personen” mit
  - Zertifikat der DFN-PKI Global
  - Schriftlicher Ernennung durch die Anwender-Einrichtung

Scan-Auftrag erstellen

Übersicht Scan-Ergebnisse

DFN Deutsches Forschungsnetz

Name Ihrer Einrichtung: HS Musterstadt

Auftragserstellung	Scanbeginn	Auftragsende	Netzbereich	Scantyp	Status	
08.02.2010 16:40	08.02.2010 16:41	08.02.2010 16:46	192.168.42.0/24	Standardscan	Fertig	
09.02.2010 09:13	09.02.2010 09:13	09.02.2010 09:17	192.168.0.0/24	Standardscan	Fertig	
09.02.2010 17:12	09.02.2010 17:13	09.02.2010 17:13	172.16.12.13	Tiefenscan	Fertig	
11.02.2010 11:39	11.02.2010 11:39	11.02.2010 11:43	172.16.0.0/24	Standardscan	Fertig	

- Über Beginn und Ende eines Scans wird per E-Mail informiert
- Je nach Netzwerk dauert ein Scan (Class C) wenige Minuten oder einige Stunden
- Die Scan-Ergebnisse werden für 90 Tage gespeichert

Scan-Ergebnisse

DFN Deutsches Forschungsnetz

Willkommen | Schwachstellen | Automatische Warnmeldungen | Netzwerkprüfer | Hilfe

Übersicht | Scan-Auftrag | Scan-Ergebnisse | Informationen

Ergebnis des Scan-Auftrags #123 über 192.168.42.0/24

IP-Adressen	
Gesamtzahl	256
Aktiv	9
Mit offenen Ports	8

Port	#TCP	#UDP
21	1	0
22	7	0
25	1	0
111	1	0
179	1	0
427	1	0
443	2	0

Filtern: Keine UDP-Ports | Gefilterte Ports nicht anzeigen | Aktualisieren

	Adresse	Portzahl	Offene TCP Ports
[+]	192.168.42.13	1	179
[+]	192.168.42.29	0	
[+]	192.168.42.110	1	22
[+]	192.168.42.231	2	22, 443

- Diese Informationen können natürlich auch Dritte aus dem Internet herausfinden.

Netzwerkprüfer zusammengefasst

- Pilotbetrieb läuft mit Tests auf verschiedenen Ebenen
  - Technik, Betrieb, organisatorische Abläufe, ...
- Verfügbar ab kommender DFN-BT (28.10.)
- Weitere Ideen in Vorbereitung
  - Schwachstellen-Scanner
  - **Scan von Grid-Firewalls** (Vortrag Timo Schäpe)
  - uvm.

Fazit

- Zusammenarbeit DFN-CERT und KIT-CERT verbessert die Unterstützung der Grid-Community

- DFN-CERT Portal - wichtiges Werkzeug für die Unterstützung der DFN-Anwender
  - Konsolidierung der Informationsangebote in eine einheitliche Portal-Struktur
  - Mechanismen zur Konfiguration der Dienste
  - “Punktgenaue” Vorfilterung der Informationen

- Grid-Community kann vom DFN-CERT Portal profitieren, insbesondere durch
  - Informationen zu Schwachstellen in Grid-Systemen
  - Scan von Grid-Firewalls

Kontakt

- Wenn Sie an den DFN-CERT Diensten teilnehmen wollen, sprechen Sie uns an

✓ **Web:** http://www.cert.dfn.de

✓ **Portal:** https://portal.cert.dfn.de

✓ **Fragen zu den DFN-CERT-Diensten:**

cert@dfn.de