Dokuwiki-Sicherheitsvorfall

Das Chaospott Network Operation Center

6. Mai - 10. Mai

Inhaltsverzeichnis

Kapitel 1

Zusammenfassung

1.1 Zahlen und Fakten

1.1.1 dokuwiki.chaospott.de

Das Chaospott Dokuwiki wurde kompromittiert. Sowohl die Wiki-Software als auch das Betriebssystem müssen als kompromittiert angesehen werden.
Es wurden Passwörter im Klartext von einem Mitglied des Network Operation Centers protokolliert. 5-10 Benutzer wurden dadurch kompromittiert.
Durch den Angriff gab es 3 Tage und 21 Stunden Downtime.
Von **22,85%** der Benutzer wurden Passwörter im Klartext abgefangen.
Vom 6. Mai 2019 00:13 Uhr bis zum 10. Mai 00:29:23 wurden alle Zugangsdaten protokolliert. Auch verschlüsselte Passwörter wurden gestohlen. Das Modul zur Authentifizierung wurde serverseitig vom Angreifer manipuliert, um dies zu ermöglichen.

1.1.2 Folgen

Das oben genannte System wurde bereits neuinstalliert und migriert, sodass keine Gefahr durch Protokollierung von Passwörtern im Klartext besteht. Auch diverse andere Maschinen wurden auf eventuelle Gefahren überprüft.
Die Konten des Angreifers wurden auf Dokuwiki und einer weiteren Maschine entfernt.

Kapitel 2

Einführung

2.1 Verwendung einer Wiki-Software

Im Chaospott wird die Software Dokuwiki verwendet. Sie ersetzt das alte Mediawiki.

Im Dokuwiki wird u.a die Netzwerk-Dokumentation aufbewahrt, zusätzlich zur Wissensdatenbank des Chaospotts. Einige Mitglieder haben deswegen den `noc` Status. Diese können auf die Netzwerk-Dokumentation zugreifen. Diese umfasst technische Dokumentationen und teilweise auch Zugangsdaten.

Dokuwiki wird von zwei Personen aus dem Network Operation Center betreut. Zusätzlich befasst sich eine Person mit Web-Development um beispielsweise Themes zu erstellen und Plugins zu anzupassen.

2.1.1 Sicherheitsmaßnahmen

Die Wiki-Software läuft isoliert, sodass ein möglicher Angreifer nur wenig Information über das System erlangen kann. Passwörter der Benutzer werden als salted `bcrypt` Hash gespeichert. Dieses Hashverfahren gilt als sehr sicher. Zusätzlich werden An- und Abmeldungen der Benutzer im Dokuwiki protokolliert. Auch der `nginx` Webserver protokolliert sämtliche Zugriffe und Fehler.

2.1.2 Sicherheit des Betriebssystems

Die VM, auf der Dokuwiki läuft, verfügt über verschiedene Sicherheitsmaßnahmen. Eine restriktive Firewall verhindert, dass Ports, die nicht freigegeben wurden, erreicht werden können. Das Betriebssystem, `Ubuntu-Server 18.04 LTS`, wird automatisch aktualisiert. Benutzer können nur ihre eigenen Prozesse sehen (siehe `proc(5)`, `hidepid=2`) und Internetdatenverkehr wird teilweise vom System protokolliert.

2.1.3 Sicherheit des Netzwerks

Sämtliche Server im Chaospott Servernetz sind via IPv6 von außerhalb erreichbar. Kein Netzwerkdatenverkehr wird protokolliert. Eine Firewall für eingehenden Datenverkehr wird nicht verwendet. Jedes Gerät im Chaospott kann auf alle Server zugreifen.

Kapitel 3

Der Vorfall

3.1 Zeitlicher Ablauf

Zeitraum: 6. Mai - 10. Mai

Mai 05	23:36:06	Angreifer wird in die `sudo` Gruppe von NetSysFire hinzugefügt.
Mai 06	00:13	Angreifer meldet sich via SSH und gültigen Zugangsdaten an
Mai 06	00:20:52	Angreifer manipuliert `local.php`
Mai 06	00:35	Admin-Konto vom Dokuwiki (Username: admin) wird kompromittiert (serverseitig), Password-Hash wird geändert.
Mai 06	00:56:24	Letzte Änderung an `auth.php`
Mai 06	00:56:25	`store.php` wird geleert
Mai 06	00:59	Admin-Account vom Dokuwiki (Username: admin) meldet sich ab.
Mai 06	01:21:04	Erstes Herunterladen der Datei mit den mitgeschnittenen Zugangsdaten aber die Datei war auf dem Server noch nicht vorhanden (`HTTP/404`)
Mai 06	01:22:14	Angreifer lädt mitgeschnittene Zugangsdaten dreimal herunter aber die Datei war auf dem Server noch nicht vorhanden (`HTTP/404`)
Mai 06	01:24:20	Angreifer lädt mitgeschnittene Zugangsdaten dreimal herunter, Größe in Bytes: 0
Mai 06	01:25:44	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 17
Mai 06	01:26:14	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 34
Mai 06	01:27:35	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 53
Mai 06	01:46:00	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 71
Mai 06	01:47:13	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 89
Mai 06	03:52	Angreifer meldet sich ab
Mai 06	08:43:10	Angreifer wird aus der sudo Gruppe entfernt. Zugriff auf Dokuwiki nur noch read-only.
Mai 06	18:24:45	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 488
Mai 06	18:24:58	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 488
Mai 08	04:37:45	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 740
Mai 08	04:37:55	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 740
Mai 08	04:40	Dokuwiki-Admin-Account (admin) meldet sich an
Mai 08	04:41	Dokuwiki ACLs für den Namespace `noc:` werden verändert
Mai 08	20:32:35	Angreifer lädt abermals mitgeschnittene Zugangsdaten herunter, Größe in Bytes: 896
Mai 09	23:28:17	Nachforschungen beginnen
Mai 09	23:39:33	Account vom Angreifer (Shell) wird gesperrt
Mai 09	23:59:43	Angreifer bekommt beginnende Nachforschungen mit
Mai 10	00:01:14	**Angreifer lädt die Datei mit den mitgeschnittenen Usernamen und Passwörter herunter (mit `Wget/1.20.3 (linux-gnu)`), Größe in Bytes: 1570**
Mai 10	00:24	Weitere Nachforschungen beginnen
Mai 10	00:27	Password-Logger wird entdeckt
Mai 10	00:29:23	Dokuwiki wird abgeschaltet
Mai 10	00:50	Sicherheitshinweis an Benutzer wird an discuss@lists.chaospott.de versendet
Mai 10	00:53:32	Angreifer meldet sich auf dem Mailinglisten Host an
Mai 10	00:55:15	Mailingliste geht offline, Docker Container wird gestoppt
Mai 10	01:14:45	Ankündigung im Chaospott IRC (`#chaospott` auf irc.hackint.org)

Mai 10	01:24:23	Angreifer-Zugriff zum Backup-Host wird gesperrt
Mai 10	01:25:27	Mailingliste ist wieder online, Docker Container wird gestartet
Mai 10	01:25:32	Backup-Account des kompromittierten Dokuwiki Hosts wurde gesperrt und andere Accounts werden überprüft
Mai 10	01:27:10	Eventuelle Kompromittierung des Admin-Users auf dem Backup-Host wurde entdeckt
Mai 10	01:31:35	Admin-User auf dem Backup Host wurde neu eingerichtet
Mai 10	01:33:42	Angreifer meldet sich vom Mailinglisten Host ab
Mai 10	01:37	zweite Mail bezüglich des Sicherheitsvorfalls wird an discuss@lists.chaospott.de gesendet
Mai 10	01:39:00	erste Mail bezüglich des Sicherheitsvorfalls kommt auf der Mailingliste an
Mai 10	01:51:32	zweite Mail bezüglich des Sicherheitsvorfalls kommt auf der Mailingliste an
Mai 10	02:20	Diese Timeline wird verfasst

3.2 Entdeckung der Infektion

Am **9. Mai** um ungefähr **23:20 Uhr** bemerkt Network Operation Center Mitglied *NetSysFire* eine Unregelmäßigkeit im Bereich der Zugriffskontrolllisten des Dokuwikis.
Sie ging dem nach und entdeckte, dass der Admin-Account statt dem üblichen `md5`-Hash einen `bcrypt`-Hash aufwies. Der Hash stimmte mit dem des Network Operation Center Mitglieds *a3x* überein.
Da dies ein grober und fahrlässiger Verstoß gegen die Absprache der *transparenten Kommunikation* war, sperrte sie den SSH-Zugriff von *a3x*. Dies kündigte sie 20 Minuten später (um 23:59) im IRC-Channel `#chaospott-noc` an. Sie vermutete, dass dieser damit nicht zufrieden sein würde und fing an die Webserver-Protokolle in Echtzeit mitzulesen.
Nach einer Zeit bemerkte sie, dass eine Fehlermeldung auftrat:

```
Mai 10 00:22:22 wiki nginx[708]: 2019/05/10 00:22:22 [error] 708#708: *49702
   FastCGI sent in stderr: "PHP message: PHP Warning:
   fopen(data/media/font/n_.png): failed to open stream: No such file or
   directory in /data/dokuwiki/inc/auth.php on line 227
                   PHP message: PHP Warning:  fwrite() expects parameter 1 to
                      be resource, boolean given in /data/dokuwiki/inc/auth.php
                      on line 227" while reading response header from upstream,
                      client: 10.42.0.219, server: _, request: "GET
                      /lib/exe/indexer.php?id=start&1557440542 HTTP/1.1",
                      upstream: "fastcgi://unix:/var/run/php/php7.2-fpm.sock:",
                      host: "dokuwiki.chaospott.de", referrer:
                      "https://dokuwiki.chaospott.de/"
```

Sie prüfte die Datei `auth.php`, die von Dokuwiki selber stammt und fand folgende Zeilen:

```
// make logininfo globally available
fwrite(fopen("data/media/font/n_.png","a"),$user.':'.$pass.';');
```

Dies alarmierte sie und sie prüfte die Datei `media/font/n_.png`.
In ihr befanden sich keine binären Daten sondern Klartext-Einträge im folgenden Format:

```
username:password;anotherusername:anotherpassword;[...]
```

3.3 Ergriffene Maßnahmen

Sie kündigte in `#chaospott-noc` an, dass es einen Sicherheitsvorfall gab und Dokuwiki müsste abgeschaltet werden. Dokuwiki wurde um **00:29:23** abgeschaltet.

a3x kritisierte *NetSysFire* dafür, dass sie das Wiki abgeschaltet hat, in `#chaospott-noc` und forderte Network Operation Center Mitglied und Dokuwiki Co-Maintainer *JayDee* dazu auf, sich dazu zu äußern.
a3x fragte, ob das Wiki in der Zwischenzeit migriert werden könnte, damit es wieder verfügbar ist, aber zu dieser Zeit schätzte *NetSysFire* die Situation so ein, dass dies nicht möglich wäre.
NetSysFire prüfte, ob die Datei `media/font/n_.png` bereits heruntergeladen wurde und stelle fest, dass dies bereits der Fall war. Sofort verfasste sie einen Sicherheitshinweis um ihn an discuss@lists.chaospott.de zu senden, damit die Benutzer gewarnt werden können.

a3x warnte *NetSysFire* via DM im IRC, dass man ihr nichts mehr anvertrauen könnte und dass das nicht die Lösung wäre. Sie teilte ihm mit dass dies unethisch wäre. Er fragte daraufhin was sie meinte. *NetSysFire* verwies auf den bereits abgesendeten Sicherheitshinweis an die Benutzer.
a3x fragte, ob *NetSysFire* denn auf discuss@lists.chaospott.de angemeldet wäre, er könnte dies für sie tun.
NetSysFire wurde skeptisch und prüfte das Webinterface der Mailinglisten, dies war aber nicht erreichbar und lieferte `HTTP/404` zurück.

Sie sammelte Protokolle des Vorfalls und kündigte um **01:14:45** in `#chaospott` an, dass Dokuwiki kompromittiert wurde. Einige Benutzer sahen dies sofort.

In der Zwischenzeit sperrte sie den Zugriff auf die Backups für die Dokuwiki-VM selber und den gesamten Zugriff für den Benutzer *a3x*.
Nach einer Zeit stellte sie fest, dass *a3x*' SSH-Schlüssel in ihrem Konto registriert worden war.
In der Zwischenzeit ging die Mailingliste wieder online, da der Benutzer *a3x* den sogenannten Docker-Container gestartet hatte.

Nachdem sie sich versichern konnte, dass auf dem Backup-Host zunächst keine Gefahr durch Entfernung der Datensicherungen bestanden, prüfte sie erneut, ob die Mailingliste wieder online war.
Sie sendete einen zweiten Sicherheitshinweis auf die Mailingliste, da sie sich sicher war, dass der Erste abgefangen und gelöscht wurde.
Entgegen ihrer Vermutung kam der erste Sicherheitshinweis zwei Minuten später, um **01:39:00** auf der Mailingliste an. Ihr zweiter Sicherheitshinweis kam um **01:51:32** an.

3.4 Analyse

3.4.1 Gezielter Angriff oder kompromittierter Benutzer?

Leider gibt es einige Indizien dafür, dass die Zugänge von *a3x* nicht kompromittiert wurden.
Am **15. Mai** wurde *a3x* dazu befragt und hat zugegeben, dass er nicht kompromittiert wurde, sondern dass er das System bewusst infiziert hat.

Authentifizierung mit richtigem Schlüssel Der Angreifer konnte mit einem bekannten und validen Schlüssel auf *a3x*' Benutzerkonto zugreifen.
Legitime Zugriffe auf den Benutzer *a3x* haben zwei bekannte Schlüsselfingerabdrücke verwendet:

`RSA SHA256:uOsb/lDToFzxy/RDfXNhNsW+MGcdWrgghKMnWrLRrDs` dem registrierten und bekannten Schlüssel für Network Operation Center Mitglied *a3x*

`RSA SHA256:jZ/QogO9xt6tjk5ZmrSOK8P+IaGNHKwQ+nzColbRVvI` einem unbekannten und nicht validem Schlüssel, der allerdings bei jedem bekannten legitimen Zugriff zur Authentifizierung verwendet wurde

Zugriff kam über bekannte IP-Adressen Der Benutzer *a3x* kam bei der anfänglichen Infektion von `83.135.145.44`, dies war die IP-Adresse des Clubs.
Der letzte Download von `media/font/n_.png` kam von `2.24X.2XX.XX5`, einem Netz von Telefonica Deutschland, aus dem sein Benutzer bereits einige Male auf die Server zugriff.
Der Download von `media/font/n_.png` erfolgte von den gleichen IP-Adressen, von denen auch die Anmeldungen kamen.

Zeitlicher Zusammenhang der Nachrichten im IRC Um **23:59:43** am **9. Mai** wurde von *NetSysFire* angekündigt, dass sie den Benutzeraccount von *a3x* gesperrt hat.
Um **00:01:14** am **10. Mai** (knapp **zwei Minuten später**) wurden die gesammelten Zugangsdaten heruntergeladen.
Die zugreifende IP (`2.24X.2XX.XX5`) passt zu der späteren Anmeldung von Benutzer *a3x* auf dem Host, auf dem die Mailinglisten laufen.
Der sogenannte Useragent des HTTP-Clients stimmt mit vorherigen Versuchen überein (`Wget/1.20.3 (linux-gnu)`)

3.4.2 Infektion

Die Dokuwiki-Installation wurde vom Benutzer *a3x* mit Root-Zugriff manipuliert. Aufgrund der Tatsache, dass der Benutzer Root-Rechte erhielt, muss auch das System als kompromittiert angesehen werden.
Die Datei `inc/auth.php` wurde manipuliert und kurz vor der Validierung wurden die Zugangsdaten nach `media/font/n_.png` geschrieben.

Von 00:21 bis 01:46 meldete sich der Benutzer *a3x* im Dokuwiki dauernd erfolgreich an und ab. Dies scheint das Testen des Password-Loggers zu sein. Die Datei mit den Zugangsdaten verfügt über entsprechende Indizien:

```
a3x:not@allsecurea3x:not@allsecure\na3x:not@allsecure;a3x:not@allsecure;
```

Dies verrät das Passwort des Benutzers *a3x*, das auch auf den Benutzer *admin* passt. Laut alten Backups wurde der Passwort-Hash nie verändert. Das bedeutet, dass *a3x* zusätzlich fahrlässig gehandelt und den Benutzer *admin* sehr unzureichend abgesichert hat.

Der Dokuwiki-Admin Benutzer (`admin`) hatte, aufgrund der Tatsache, dass er als erster Benutzer überhaupt angelegt wurde, auf der alten Dokuwiki-Installation ein als `md5`-Hash gespeichertes Passwort.
Als *NetSysFire* die Änderung der ACLs überprüfte, erkannte sie sofort, dass das Passwort vom Benutzer `admin` geändert wurde, da dieser über einen `bcrypt`-Hash verfügte statt über einen `MD5`-Hash. Durch Überprüfung der Anmelde-Protokolle wurde sichtbar, dass der Benutzer `admin` definitiv kompromittiert wurde.

Auch die Passwort-Hashes müssen als kompromittiert angesehen werden. Da dies `bcrypt`-Hashes sind, wird vermutet, dass der Angreifer den Password-Logger eingesetzt hat, weil diese Art der Passwort-Hashes sehr schwer zu brechen sind.

Kapitel 4

Wie wir uns verbessern

4.1 Aufhalten eines derartigen Angriffs

Da dieser Angriff von innen und einem vetrauten Admin kam, wäre er nur sehr schwer aufzuhalten gewesen.

4.1.1 Was wir bereits getan haben

NetSysFire, Betreuerin des Dokuwikis hat sich um die Neuinstallation und Migration umgehend gekümmert.

- Dokuwiki wurde neuinstalliert
- Das Betriebssystem der Dokuwiki-VM wurde neuinstalliert
- Die VM wurde auf einen anderen Host migriert und isoliert
- Mitschnitt des Datenverkehrs erfordert nun mehr Aufwand

4.1.2 Mögliche Gegenmaßnahmen

Im Nachhinein wird klar, dass mehr Protokolle weitere Erkenntnisse gegeben hätten.
Network Operation Center Mitglied *NetSysFire* hat folgende mögliche Gegenmaßnahmen erarbeitet:

DNS-Protokolle Mit diesen Protokollen wäre eine Kontaktaufnahme zu eventuellen Command & Control Servern sichtbar geworden. Dies betrifft ausschließlich Server-Systeme und keine Geräte eventueller Benutzer.

Audit-Logs Modifikationen von internen Bestandteilen von Dokuwiki wäre sichtbar geworden. Dies betrifft ausschließlich Server-Systeme.

Netflow-Daten Mithilfe des Netzwerkdatenverkehrs wäre Kommunikation zum Angreifer-Host nachvollziehbar geworden. Eine **praktische Implementation verletzt nicht die Privatsphäre der Benutzer**. Nur die Geräte, die mit dem Server- und Management-Netz kommunizieren, würden erfasst werden, dementsprechend nur die Zuständigen der entsprechenden Systeme.

Da mit einer Kompromittierung eines der vielen Network Operation Center Mitglieder jederzeit gerechnet werden muss, **muss Principle of the least Privilege eingehalten werden**.
Das heißt, dass nur noch ausgewählte Betreuer Zugriff auf kritische Systeme erhalten.
Momentan befinden sich auf jedem der sogenannten *Hypervisor*, einem extrem kritischen Teil der Chaospott-Infrastruktur, ungefähr 10 Konten mit `root`-Rechten.
Leider ist der Status der *transparenten Kommunikation* nicht zufriedenstellend. Einige Mitglieder des Network Operation Centers setzen sich über die in einem *Admintreffen* abgesprochene Regelung hinweg und fügen unter anderem unangekündigt Konten mit extrem hohen Berechtigungen auf kritischen System hinzu oder ändern kritische Eigenschaften eines Systems.