

Re: Apache Software Foundation Server compromised, resecured. (fwd)

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-06/3215.html>

From: Karsten W. Rohrbach (karsten@rohrbach.de)

Date: 06/01/01

Date: Fri, 1 Jun 2001 01:27:52 +0200

From: "Karsten W. Rohrbach" <karsten@rohrbach.de>

To: Cy Schubert - ITSD Open Systems Group <Cy.Schubert@uumail.gov.bc.ca>

this was one "result" of the comromised ssh binary at sourceforge.

i don't want to think about it aloud in public what's next :-(

last | grep sourceforge

for (every account affected)

pw usermod "account" -h -

sh*t

/k

Cy Schubert – ITSD Open Systems Group(Cy.Schubert@uumail.gov.bc.ca)@2001.05.31 16:00:17 +0000:

> *Some of you might be interested in this.*

>

>

> *Regards, Phone: (250)387-8437*

> *Cy Schubert Fax: (250)387-5766*

> *Team Leader, Sun/Alpha Team Internet: Cy.Schubert@osg.gov.bc.ca*

> *Open Systems Group, ITSD, ISTA*

> *Province of BC*

>

>

> ----- *Forwarded Message*

>

> *Date: Wed, 30 May 2001 23:05:59 -0700 (PDT)*

> *From: Brian Behlendorf <brian@apache.org>*

> *X-X-Sender: <brian@localhost>*

> *To: announce@apache.org*

> *Subject: Apache Software Foundation Server compromised, resecured.*

> *Message-ID: <Pine.BSF.4.31.0105302301190.41134-100000@localhost>*

> *MIME-Version: 1.0*

> *Content-Type: TEXT/PLAIN; charset=US-ASCII*

> *X-Spam-Rating: h31.sny.collab.net 1.6.2 0/1000/N*

>

>

FreeBSD–Security: Re: Apache Software Foundation Server compromised, resecured. (fwd)

- > *Earlier this month, a public server of the Apache Software Foundation*
- > *(ASF) was illegally accessed by unknown crackers. The intrusion into*
- > *this server, which handles the public mail lists, web services, and*
- > *the source code repositories of all ASF projects was quickly*
- > *discovered, and the server immediately taken offline. Security*
- > *specialists and administrators determined the extent of the intrusion,*
- > *repaired the damage, and brought the server back into public service.*
- >
- > *The public server that was affected by the incident serves as a source*
- > *code repository as well as the main distribution server for binary*
- > *release of ASF software. There is no evidence that any source or binary*
- > *code was affected by the intrusion, and the integrity of all binary*
- > *versions of ASF software has been explicitly verified. This includes*
- > *the industry–leading Apache web server.*
- >
- > *Specifically: on May 17th, an Apache developer with a sourceforge.net*
- > *account logged into a shell account at SourceForge, and then logged*
- > *from there into his account at apache.org. The ssh client at*
- > *SourceForge had been compromised to log outgoing names and passwords,*
- > *so the cracker was thus able get a shell on apache.org. After*
- > *unsuccessfully attempting to get elevated privileges using an old*
- > *installation of Bugzilla on apache.org, the cracker used a weakness in*
- > *the ssh daemon (OpenSSH 2.2) to gain root privileges. Once root, s/he*
- > *replaced our ssh client and server with versions designed to log names*
- > *and passwords. When they did this replacement, the nightly automated*
- > *security audits caught the change, as well as a few other trojaned*
- > *executables the cracker had left behind. Once we discovered the*
- > *compromise, we shut down ssh entirely, and through the serial console*
- > *performed an exhaustive audit of the system. Once a fresh copy of the*
- > *operating system was installed, backdoors removed, and passwords*
- > *zeroed out, ssh and commit access was re–enabled. After this, an*
- > *exhaustive audit of all Apache source code and binary distributions*
- > *was performed.*
- >
- > *The ASF is working closely with other organizations as the investigation*
- > *continues, specifically examining the link to other intrusion(s), such*
- > *as that at SourceForge (<http://sourceforge.net/>) [and php.net*
- > *(<http://www.php.net/>).]*
- >
- > *Through an extra verification step available to the ASF, the integrity*
- > *of all source code repositories is being individually verified by*
- > *developers. This is possible because ASF source code is distributed*
- > *under an open–source license, and the source code is publicly and freely*
- > *available. Therefore, the ASF repositories are being compared against*
- > *the thousands of copies that have been distributed around the globe.*
- > *While it was quickly determined that the source code repositories on the*
- > *ASF server were untouched by the intruders, this extra verification step*
- > *provides additional assurance that no damage was done.*
- >
- > *As of Tuesday, May 29, most of the repository has been checked, and as*
- > *expected, no problems have been found. A list of verified modules*

FreeBSD–Security: Re: Apache Software Foundation Server compromised, resecured. (fwd)

> *will be maintained, and is available here:*
> <http://www.apache.org/info/hack-20010519.html>
>
> *Because of the possible link of the ASF server intrusion to other
> computer security incidents, the investigation is ongoing. When
> complete, the ASF will offer a complete and public report.*
>
> *The Apache Software Foundation strongly condemns this illegal
> intrusion, and is evaluating all options, including prosecution of the
> individual(s) responsible to the fullest extent of the law. Anyone
> with pertinent information relating to this or other related events
> should contact root@apache.org. Anyone from the media with further
> interest should contact press@apache.org.*
>
> *Thanks.*
>
> *Brian Behlendorf*
> *President, Apache Software Foundation*
>
>
>
>
> –

> *You have received this mail because you are subscribed to the
> announce@apache.org mailing list.
> To unsubscribe, e-mail: announce-unsubscribe@apache.org
> For additional commands, e-mail: announce-help@apache.org*
>
>

> ----- End of Forwarded Message
>
>
>
>

> *To Unsubscribe: send mail to majordomo@FreeBSD.org
> with "unsubscribe freebsd–security" in the body of the message*

--
> Unix is very simple, but it takes a genius to understand the
> simplicity. --Dennis Ritchie
KR433/KR11-RIPE -- WebMonster Community Founder -- nGENn GmbH Senior Techie
<http://www.webmonster.de/> -- <ftp://ftp.webmonster.de/> -- <http://www.ngenn.net/>
karsten@rohrbach.de -- alpha@ngenn.net -- alpha@scene.org -- catch@spam.de
GnuPG 0x2964BF46 2001-03-15 42F9 9FFF 50D4 2F38 DBEE DF22 3340 4F4E 2964 BF46

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd–security" in the body of the message

- application/pgp–signature attachment: [stored](#)