

[UNIX] qwik-smtpd Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0016.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/03/04

To: list@securiteam.com

Date: 3 Nov 2004 17:58:08 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

qwik-smtpd Format String Vulnerability

SUMMARY

The <<http://qwikmail.sourceforge.net/smtpd/>> QwikMail SMTP server (qwik-smtpd) is "a fast, secure, and efficient mail server (MTA). It is written in C and many security precautions have been taken to ensure that the code is safe".

A format string vulnerability exists in the product's logging routine that allows a remote attacker to cause the product to execute arbitrary code.

DETAILS

Vulnerable Systems:

* qwik-smtpd version 0.3

Vulnerable code:

In the file qwik-smtpd.c the following can be found:

```
sprintf(Received,"Received: from %s (HELO %s) (%s) by %s with SMTP; %s\n",
clientHost, clientHelo, clientIP, localHost, timebuf);
```

```
..
```

```
    else
    {
```

Securiteam: [UNIX] qwik-smtpd Format String Vulnerability

```
fprintf(fpout,Received);
```

..

As you can see, bug found in main() function.

Vendor patch:

A vendor patch is available from:

<http://qwikmail.sourceforge.net/smtpd/qwik-smtpd-0.3.patch>

<http://qwikmail.sourceforge.net/smtpd/qwik-smtpd-0.3.patch>

```
--- qwik-smtpd-0.3.orig/qwik-smtpd.c 2002-06-27 22:35:24.000000000
-0700
```

```
+++ qwik-smtpd.c 2004-10-30 19:56:14.579287608 -0700
```

```
@@ -208,7 +208,7 @@
```

```
    for(x = 0; x < max_recipients; x++)
```

```
    {
```

```
        if(clientRcptTo[x] == NULL) break;
```

```
- fprintf(fpout,clientRcptTo[x]);
```

```
+ fprintf(fpout,"%s", clientRcptTo[x]);
```

```
    (void) fflush(fpout);
```

```
    fprintf(fpout,"\n");
```

```
    (void) fflush(fpout);
```

```
@@ -431,9 +431,9 @@
```

```
    }
```

```
    else
```

```
    {
```

```
- fprintf(fpout,Received);
```

```
+ fprintf(fpout,"%s", Received);
```

```
    (void) fflush(fpout);
```

```
- fprintf(fpout,messageID);
```

```
+ fprintf(fpout,"%s", messageID);
```

```
    (void) fflush(fpout);
```

```
    out(354, "type away!");
```

```
    alarm(data_timeout);
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:darkeagle@list.ru> Dark Eagle.

The original article can be found at:

<<http://unl0ck.info/advisories/qwik-smtpd.txt>>

<http://unl0ck.info/advisories/qwik-smtpd.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [UNIX] qwik-smtpd Format String Vulnerability

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.