[UNIX] Samba FindNextPrintChangeNotify Error Allows Remote Authenticated Users To Crash smbd

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2004−09/0015.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 09/06/04

```
To: list@securiteam.com
Date: 6 Sep 2004 14:05:55 +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/mailinglist.html

− − − − − − − − −

Samba FindNextPrintChangeNotify Error Allows Remote Authenticated Users To Crash smbd
−−−

crash. The behaviour can be triggered easily by a Windows XP SP2 client
which apparently does this in certain situations.

The flaw is located in the printer_notify_info() in
'rpc_server/srv_spoolss_nt.c' .

Vendor Status:
The vulnerability was reported to the vendor by Craig Huegen. The vendor
has already issued a new upgrade version which is available from
<http://samba.org/samba/download/> http://samba.org/samba/download/.

ADDITIONAL INFORMATION

The information has been provided by <mailto:jerome.athias@caramail.com>
"JXrXme" ATHIAS.

==========

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

==========
==========

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.