

# [TOOL] crypt\_blowfish – Modern Password Hashing Algorithm for Crypt

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00030.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 8 Feb 2006 18:58:27 +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>

-----

crypt\_blowfish – Modern Password Hashing Algorithm for Crypt

---

## SUMMARY

## DETAILS

crypt\_blowfish is a public domain implementation of a modern password hashing algorithm based on the Blowfish block cipher, provided via the crypt(3) and a reentrant interface. It is compatible with bcrypt (version 2a) by Niels Provos and David Mazieres, as used in OpenBSD.

The most important property of bcrypt (and thus crypt\_blowfish) is that it is adaptable to future processor performance improvements, allowing you to arbitrarily increase the processing cost of checking a password while still maintaining compatibility with your older password hashes. Already now bcrypt hashes you would use are several orders of magnitude stronger than traditional Unix DES-based or FreeBSD-style MD5-based hashes.

## ADDITIONAL INFORMATION

[TOOL] crypt\_blowfish – Modern Password Hashing Algorithm for Crypt

The information has been provided by <<mailto:solar@xxxxxxxxxxxxx>> Solar Designer.

For the latest version of this tool visit the project's homepage at:  
<<http://www.openwall.com/crypt/>> <http://www.openwall.com/crypt/>

=====

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@xxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxx)

=====

=====

**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.