

[NEWS] Dell BIOS DoS (Invalid Characters in BIOS Password)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0029.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/09/03

To: list@securiteam.com

Date: 9 Dec 2003 10:30:58 +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>

Dell BIOS DoS (Invalid Characters in BIOS Password)

SUMMARY

The Dell BIOS allows users to set several different passwords to protect their machines from unauthorized access. There is:

- 1) A Setup Password, which is required to enter the BIOS setup, as well as
- 2) A Hard Drive Password, as per the ATA Security Feature Set Specification

Due to a bug in the BIOS, a password containing characters that cannot be later entered, can be provided by a user. This allows a local user to create a denial of service (as the password authentication mechanism cannot be bypassed) situation.

DETAILS

Affected Systems:

Dell Inspiron 2650 System BIOS, A11 (A11 is the current BIOS as of writing, and was released in late September of this year)

Unfortunately, once a Hard Drive Password is set which contains one or more of the following characters , < > . ; : ' [] { } .

Securiteam: [NEWS] Dell BIOS DoS (Invalid Characters in BIOS Password)

It can not be later entered to access the machine. It appears as though a bug in the BIOS code prevents those characters from being taken as input when the user is asked for the password – however, the BIOS incorrectly allows users to set passwords containing those characters.

This is not an incredibly serious problem as such, since a user can go back into the BIOS setup and change the password there, provided the BIOS Setup is not protected with an unknown password. Or, as a last resort, Dell can be phoned to provide a master backdoor password, as long as the user can prove that he is the legal owner of the computer. Of course, the prerequisite of physical access to the machine highly mitigates this vulnerability.

It is however an interesting bugs from the point of view of Dell's practices. James has contacted them over two weeks ago, but their 'technical support' is unable to understand or resolve the problem. Two of their representatives told me to reinstall Windows XP Chipset drivers, even when James asked to be forwarded to people higher in the technical support chain. Perhaps this post will encourage Dell to pay more attention in the future.

ADDITIONAL INFORMATION

The information has been provided by <mailto:jae7@lehigh.edu> James Evans.

=====

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.