

[NT] St. Bernard Open File Manager Heap Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00046.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 18 Dec 2007 18:40:59 +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>

St. Bernard Open File Manager Heap Overflow Vulnerability

SUMMARY

A vulnerability allows attackers to execute arbitrary code on vulnerable installations of St. Bernard Open File Manager. Authentication is not required to exploit this vulnerability.

DETAILS

Vulnerable Systems:

- * Open File Manager version 9.5

Immune Systems:

- * Open File Manager version 9.6 build 602

The specific flaw resides in the Open File Manager service, ofmnt.exe, which listens by default on a random TCP port near 1000. The process blindly copies user-supplied data to a static heap buffer. By supplying an overly large amount of data, an attacker can overflow that buffer leading to arbitrary code execution in the context of the SYSTEM user.

Vendor Response:

[NT] St. Bernard Open File Manager Heap Overflow Vulnerability

St. Bernard has issued an update to correct this vulnerability. Version 9.6 build 602 available to customers addresses this issue. Other affected vendors such as Hewlett-Packard have made fixes available to customers as well.

Disclosure Timeline:

2007.07.20 – Vulnerability reported to vendor
2007.12.17 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6281>>
CVE-2007-6281

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>
The Zero Day Initiative (ZDI).
The original article can be found at:
<<http://www.zerodayinitiative.com/advisories/ZDI-07-078.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-078.html>

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.