

[NEWS] EMC Navisphere Manager Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0023.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/07/05

To: list@securiteam.com

Date: 7 Aug 2005 17:15:39 +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>

EMC Navisphere Manager Directory Traversal

SUMMARY

" <http://www.emc.com/products/storage_management/navisphere.jsp> EMC Navisphere storage management software is a suite of tools that enables discovery, monitoring, provisioning, and reporting on EMC CLARiiON FC4700 Storage Systems."

EMC Navisphere Manager does not properly filter incoming requests and as such is vulnerable to a directory traversal vulnerability.

DETAILS

Vulnerable Systems:

- * Navisphere Manager Base version 6.4.1.0.0

Immune Systems:

- * Management Server version 6.6.0.5.0
- * Management Server Base version 6.6.0.5.0
- * Windows Management Server version 6.6.0.5.0
- * Management Server version 6.5.4.0.0
- * Management Server Base version 6.5.4.0.0

Securiteam: [NEWS] EMC Navisphere Manager Directory Traversal

- * Windows Management Server version 6.5.4.0.0
- * Management Server version 6.4.8.0.0
- * Management Server Base version 6.4.8.0.0
- * Windows Management Server version 6.4.8.0.0

Exploitation of a directory traversal vulnerability in EMC Navisphere Manager could allow an attacker to retrieve arbitrary files from the system running Navisphere Manager as well as retrieve directory listings.

The following request can be used to retrieve the Navisphere Manager log file, which often contains the administrative password in plain-text:

<http://vulnerable/../../../../../../../../EMC/NAVISPHERE/common/log/navimon.log>

Another flaw allows a user to list the contents of arbitrary directories by simply appending a '.' to the end of a request.

Workaround:

Limit access to the Navisphere Manager server to only trusted hosts by limiting access to trusted users only on TCP port 80.

Vendor Status:

"The vulnerability identified is found in older versions of Navisphere Management Server (r), for which an update has been issued. In these updated versions, HTTP validation is implemented. Attempts to traverse the file system by way of a URL (e.g., "../../../../") are detected and such requests are rejected with the following error:

'The page cannot be displayed'

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2357>>
CAN-2005-2357

Disclosure Timeline:

04/19/2005 – Initial vendor notification

05/05/2005 – Initial vendor response

08/05/2005 – Coordinated public

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@idefense.com>> ideoense.

The original article can be found at:

<<http://www.ideoense.com/application/poi/display?id=288&type=vulnerabilities>>
<http://www.ideoense.com/application/poi/display?id=288&type=vulnerabilities>

=====

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

Securiteam: [NEWS] EMC Navisphere Manager Directory Traversal

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.