

[NEWS] Sophos Email Security Appliance Cross Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00070.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 17 Feb 2008 08:42:59 +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>

Sophos Email Security Appliance Cross Site Scripting Vulnerability

SUMMARY

Sophos ES1000 Email Security Appliance delivers "protection against spam, viruses, Trojans, spyware and other malware. Sophos's award-winning anti-virus engine detects all types of malware in a single, high-speed scan. Every Sophos appliance is updated with new protection intelligence every 5 minutes". During an audit of Sophos ES1000 Email Security Appliance, a Cross Site Scripting vulnerability was discovered in its web administration interface. Administration web interface is available on the public network interface, over HTTPS on port 18080.

DETAILS

Vulnerable Systems:

- * Sophos ES1000 version 2.1.0.0 and prior
- * Sophos ES4000 version 2.1.0.0 and prior

Immune Systems:

- * Sophos ES1000 version 2.1.1.0
- * Sophos ES4000 version 2.1.1.0

[NEWS] Sophos Email Security Appliance Cross Site Scripting Vulnerability

Lack of input validation for 'error' and 'go' parameters of the 'Login' script, allows malicious JavaScript code injection.

<https://192.168.0.10:18080/Login?logout=0&error=<INJECTION>&go=<INJECTION>>

This can be exploited by a malicious user to steal Sophos ES1000 Email Security Appliance administrator credentials, and shut down the appliance, or change its configuration.

Fix:

This vulnerability has been fixed in Sophos Email Appliance version 2.1.1.0 and above, available automatically to Sophos' customers between 14–21 February 2008. More information at

[<http://www.sophos.com/support/knowledgebase/article/34733.html>](http://www.sophos.com/support/knowledgebase/article/34733.html)

<http://www.sophos.com/support/knowledgebase/article/34733.html>

Vendor status:

28.01.2008 – Initial contact, automated response

04.02.2008 – Repeated contact

06.02.2008 – Vendor response

07.02.2008 – Vendor status update

08.02.2008 – Vendor status update

13.02.2008 – Vendor status update

14.02.2008 – fix available

15.02.2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by [<mailto:leon.juranic@xxxxxxxxx>](mailto:leon.juranic@xxxxxxxxx) Leon Juranic.

The original article can be found at:

[<http://www.infigo.hr/en/in_focus/advisories/INFIGO-2008-02-13>](http://www.infigo.hr/en/in_focus/advisories/INFIGO-2008-02-13)

http://www.infigo.hr/en/in_focus/advisories/INFIGO-2008-02-13

=====

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@xxxxxxxxxxxxxxxx

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

=====
=====

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,

[NEWS] Sophos Email Security Appliance Cross Site Scripting Vulnerability

loss of business profits or special damages.