

[NT] Level Platforms Service Center Install Data HTTP Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00024.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 10 Feb 2008 19:53:40 +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>

Level Platforms Service Center Install Data HTTP Vulnerability

SUMMARY

Level Platforms, Inc. (LPI) flagship product Managed Workplace Service Center, which provides remote monitoring, reporting and alerting of device & network status. The software is typically used by Managed Service Providers and large IT departments. There is also a hosted version offered through Ingram Micro.

LPI's software has two components, a Service Center (server) component, and a Onsite Manager (client) component. The Service Center is typically installed at a MSP's facility. The Service Center software sends & receives data with one or more Onsite Manager software installations (typically deployed at remote networks). The Service Center software also provides a central console for management, monitoring, reporting and alerting.

There exists at least one vulnerability in the Service Center software that allows an attacker to remotely determine a wide variety of potentially useful information via an HTTP URL.

DETAILS

[NT] Level Platforms Service Center Install Data HTTP Vulnerability

Detailed Description:

A default install of the software handling the URL:

```
"http[s]://<SERVICE CENTER NAME>/About/SC_About.htm"
```

enumerates the following information without first checking to see if the source of the command is authenticated (The <SERVICE CENTER NAME> is the name that has been assigned to the Service Center website);

- Version
- Build
- Applied service packs
- Applied Hot Fixes
- The date and time each were installed.

Exploitation of this vulnerability provides an with attacker potentially useful information that could be leveraged to attack the host, clients or other resource to which they have access.

A Google search using the phrase "/About/SC_About.htm" enumerates vulnerable systems.

No information has been provided to support any benefit achieved by making this information publically available.

Vendor Response:

This issue was reported to LPI by email on February 1, 2008.

On February 5, 2008 the following reply was received; "Thank you for your input. I have forwarded this email over to our development team for their consideration. Regards,..."

On February 6, 2008 the following reply was received; "...Our development team is aware is this particular issue, and should be addressing it, just want to let you know that having access to your build/version number isn't hazardous to your managed services business..."

Our Recommendation:

1. There is no reason to give away the version/build number and every reason to keep it confidential. Reduce the attack surface wherever possible or practical.
2. Take steps to prevent publishing or exposing any unnecessary or sensitive information that could be used to exploit your network.
3. Until the vulnerability is resolved by LPI;
 - a) Prevent or restrict IP level access to the Service Center website by restricting access to trusted IP ranges, or through VPN's. Note that preventing Onsite Manager access to the Service Center website will result

[NT] Level Platforms Service Center Install Data HTTP Vulnerability

in loss of functionality.

b) Review the security settings of each web page within Service Center.

c) Disallow indexing of the Service Center site by search engines using IP restrictions, robots.txt files or other measures

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=>> CVE-2008-0636

ADDITIONAL INFORMATION

The information has been provided by <<mailto:BPowers@xxxxxxxxxxxxxxxxx>>
Brook Powers.

The original article can be found at:

<<http://www.tech-serve.com/research/advisories/2008/>>
<http://www.tech-serve.com/research/advisories/2008/>

=====

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.