CERT Incident Note IN-99-08: Attacks Against ISS web servers involving MCAD

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Attacks against IIS web servers involving MDAC

Friday, December 10, 1999

We have received reports of IIS web servers compromised via a vulnerability in MS Data Access Components (MDAC). This vulnerability has been widely discussed as early as April 22, 1998. Here are some pointers to information about this vulnerability:

> http://support.microsoft.com/support/kb/articles/q184/3/75.asp
> http://www.microsoft.com/security/bulletins/ms98-004.asp
> http://www.microsoft.com/security/bulletins/ms99-025.asp

In incidents reported to us so far, attacks can be identified by looking through the IIS log files for POST access to the file "/msadc/msadcs.dll". For example:

```
1999-10-24 20:38:12  - WWW  POST /msadc/msadcs.dll 200 1409 664 782 ACTIVEDATA - -
```

If you use Microsoft Remote Data Services (RDS) these POST operations may be legitimate.

We encourage all sites using IIS to carefully follow the steps listed in Microsoft Advisory MS99-025, referenced above, to secure or disable RDS.