National Infrastructure Security Co-ordination Centre

cameronr@niscc.gov.uk
Product Vulnerability
Management

Tel: 020 7821 330 ext: 4520
Mb: 07789928839

NISCC/Vul/006424

02 July 2003

PO BOX 832
London
SW1P 1BG

Dear

Re: Network Protocol Security Vulnerabilities

The United Kingdom National Infrastructure Security Co-ordination Centre (NISCC) has recently become aware of security vulnerabilities in several network protocols, H323, S/Mime, SSL and X400. The weaknesses may affect products that you produce. Testing to date has reliably confirmed that a significant number of implementations from independent vendors have difficulties processing certain protocol constructs. The severity of the impact of such problems varies from product to product and vendor to vendor. In many cases products have been found to terminate abnormally, resulting in a denial of service. Failures may be exploitable by a remote attacker.

We would like to share the information we have with you and at some time in the future will ask you to sign a joint information sharing Pledge for the managing of future vulnerabilities; however to expedite the process we enclose a CD-ROM containing sample test data. You are reminded of the need to limit distribution of this sensitive information; it is not to be passed to a third party without prior permission of NISCC-UNIRAS. You will also note from the content on some of the CD's that NISCC is working in partnership with a third party, please ensure that any queries are addressed to NISCC and not the organisation who conducted the research on our behalf.

NISCC does not charge for providing this information or the test data. We do, however, request that you nominate an individual within your company with whom we can liaise over discloser time-scales and patch production. Our intention is to co-ordinate the release of the information to the public in approximately 90 days.

It is to be noted that by using NISCC test data you are agreeing to NISCC co-ordinating the release to the general public. This release will be in the form of a NISCC-UNIRAS Vulnerability Advisory on which we will include links to your patches. We will advise you of that date once we are confident that there are a high percentage of vendors ready to provide updates to their product line.

Please note that NISCC is to be informed as soon as possible if it comes to your attention that there is the possibility or actual unscheduled public release. NISCC will co-ordinate any response.

If you have any questions please feel free to contact me (my details are above). Could you confirm receipt of the enclosed data via my email address above.

Yours sincerely

Cameron Rogers
Product Vulnerability Management