Gartner

Close Window

Nimda Worm Shows You Can't Always Patch Fast Enough

19 September 2001

John Pescatore

Nimda bundles several known exploits against Internet Information Server and other Microsoft software. Enterprises with Web applications should start to investigate less-vulnerable Web server products.

News

Note Number: FT-14-5524

Related Terms: E-Mail Security; Security

Download: PDF

Nimda Worm Shows You Can't Always Patch Fast Enough

Nimda bundles several known exploits against Internet Information Server and other Microsoft software. Enterprises with Web applications should start to investigate less-vulnerable Web server products.

Event

On 18 September 2001, a new mass-mailing computer worm began infecting computers worldwide, damaging local files as well as remote network files. The w32.Nimda.A @ mm worm can spread through e-mail, file sharing and Web site downloads. For more information, visit: http://www.microsoft.com/technet/security/topics/Nimda.asp or http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html.

First Take

As a "rollup worm," Nimda bundles several known exploits against Microsoft's Internet Information Server (IIS), Internet Explorer (IE) browser, and operating systems such as Windows 2000 and Windows XP, which have IIS and IE embedded in their code. To protect against Nimda, Microsoft recommends installing numerous patches and service packs on virtually every PC and server running IE, IIS Web servers or the Outlook Express e-mail client. As the earlier Code Red worm showed, many servers and PCs running IIS Web server processes may not be obvious since they may be run as personal Web servers on the intranet but still be exposed to the Internet.

Code Red also showed how easy it is to attack IIS Web servers (see *Gartner FirstTake* FT-14-2441 "Lack of Security Processes Keeps Sending Enterprises to 'Code Red'"). Thus, using Internet-exposed IIS Web servers securely has a high cost of ownership. Enterprises using Microsoft's IIS Web server software have to update every IIS server with every Microsoft security patch that comes out — almost weekly. However, Nimda (and to a lesser degree Code Blue) has again shown the high risk of using IIS and the effort involved in keeping up with Microsoft's frequent security patches.

Gartner recommends that enterprises hit by both Code Red and Nimda immediately investigate alternatives to IIS, including moving Web applications to Web server software from other vendors, such as iPlanet and Apache. Although these Web servers have required some security patches, they have much better security records than IIS and are not under active attack by the vast number of virus and worm writers. Gartner remains concerned that viruses and worms will continue to attack IIS until Microsoft has released a completely rewritten, thoroughly and publicly tested, new release of IIS. Sufficient operational testing should follow to ensure that the initial wave of security vulnerabilities every software product experiences has been uncovered and fixed. This move should include any Microsoft .NET Web services, which requires the use of IIS. Gartner believes that this rewriting will not occur before year-end 2002 (0.8 probability).

Analytical Source: John Pescatore, Information Security Strategies

Resource ID: 340962