TruSecure and Gartner on IIS Servers

Introduction

Gartner recently issued a report suggesting that companies reconsider the use of Microsoft IIS servers. TruSecure's Russ Cooper, Editor of NTBugtraq, the leading source of Microsoft-related security intelligence, offered this comment on Gartner's report.

Gartner has continually recommended that the only way to protect Internet-connected IIS boxes is to continually patch. According to Gartner, patching appears to be something that only Microsoft customers need to do. They imply that other webservers, like Apache, don't require patching.

This premise is flawed. Not only does Apache require patching, the underlying OS it runs on must be maintained also. If you compare IIS to Apache, you compare a webserver + OS on one side while only a webserver on the other. Not a valid comparison at all.

TruSecure has continually shown that if appropriate and minimal configuration steps are taken (i.e. something that must be done to *any* Internet-connected box of any kind) IIS can be resistant to attacks long before they occur or are even conceived. In fact, knowing of a vulnerability, and therefore its patch, is not a prerequisite to preventing an attack based on that vulnerability.

Checklists and the vast majority of patches are to be used, as that's simply common sense. However, the urgency at which they need be used greatly depends on whether or not basic TruSecure Essential Practices are employed.

Gartner's analysis is largely dependent on the premise that TruSecure Essential Practices are not in use, and that administrators are unaware of even basic security principles.

Gartner FT-13-6734 - 7 May 2001

> "Enterprises that have not yet committed to IIS as their Web server software should heavily weight security as a criterion in evaluating which Web server software to use. Although IIS may come for free as part of Windows 2000, the operational costs of continually installing patches to address new IIS vulnerabilities - not to mention the cost of security incidents against IIS before it is patched - causes IIS to carry a very high total cost of ownership."

At the heart of this quote is the premise that one must continually install patches. This precludes the use of TruSecure mitigators that often make patching unnecessary, or at least not urgent, for the vast majority of patches that are released by Microsoft. Regular maintenance is crucial, and all customers need to have a plan in place to test patches on non-production servers, as well as to get them deployed in a reasonably timely fashion. However, Gartner's statement would imply this is of little value. Again, TruSecure has proven this not to be the case.

TruSecure Corporation • 13650 Dulles Technology Drive, Ste. 500. • Herndon, VA 20171-4602 • 1.888.396.8348 •
www.trus ecure.com

Gartner FT-14-2441 - 1 August 2001

> “Enterprises should recognize that any use of IIS in Internet-connected applications requires constant vigilance for security alerts, continual application of security patches, and the use of additional security products and services that quickly detect vulnerabilities and attacks against the numerous security holes in IIS.
>
> Above all, enterprises should establish processes to make sure they promptly apply all security patches to all Internet-exposed systems and replace with more secure products those that continually have vulnerabilities exposed. As long as enterprises continue to use free software and expect to get more security than they paid for, attacks like Code Red will have a high probability of either succeeding in direct attacks or eating up attention and resources as hype makes enterprises suddenly realize their vulnerability.”

Once again, TruSecure’s Alerts and Monitor provide TruSecure customers with pro-active information to avoid falling into the panic mode when new vulnerabilities are discovered or reported by the media. When Code Red was announced TruSecure quickly reminded its customers that they had been advised more than a year earlier to make a minor configuration change that completely protected their IIS systems from the direct attack Code Red employed. IIS was not any more susceptible to the side effects of Code Red (i.e. the Denial of Service the Internet saw).

According to Gartner, everyone must apply every patch immediately. This is Microsoft’s stance, but they must have that stance. They cannot afford to suggest that a given vulnerability is less important than any other, especially when there is no known attack against the vulnerability. TruSecure’s Risk Team provides our customers with expert advice and analysis. Knowing the work that certified customers have already done to their networks enables the proper and accurate assessment of the need for any new patch provided by any vendor.

As a result, TruSecure customers are not the audience to which Gartner is speaking. Gartner assumes a lack of expertise and a lack of synergistic controls.

Gartner FT-14-5524 - 19 September 2001

> “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).”

Of most important points to note in this statement is that Gartner is referring to “enterprises hit by *both* Code Red and Nimda.”

In making such a qualification, Gartner is acknowledging that any company who was hit by both of these attacks has clearly demonstrated several things:

1. They do not apply any pro-active configuration controls.

TruSecure recommended and enforced controls with its customers years in advance of these specific attacks (without any prior knowledge of the actual attacks).

2. They are not plugged into the Security Advisory food chain, or cannot understand the advisories that are released.

TruSecure’s Alerts and Monitor, coupled together with access to Security Analysts, ensure that customers fully understand and appreciate any major event.

3. They are unable to respond in a timely fashion.

If you were hit by Code Red, then in the time between this virus and Nimda you should have corrected any problems with systems that were affected by Code Red. Had that been done, Nimda would have been ineffective. Gartner recognizes that if you were hit by both, then you were unable to take the corrective measures that Code Red required to prevent it (which would have protected systems from Nimda also).

Further, Nimda revealed other weaknesses. IIS Systems that serve multiple roles may have been compromised despite being “fully patched.” This is the most crucial observation that contradicts much of what Gartner has stated about IIS. If, for cost savings reasons, an IIS server has been used also as a File and Print server, then it may have been infected with Nimda by virtue of file shares. TruSecure has long recommended a separation of functionality that would ensure that such systems are not capable of being compromised in that fashion.

Summary

TruSecure believes that an IIS system:

- Configured with very minimal fore-thought and only basic knowledge,
- Patched within the last three months according to TruSecure specific recommendations (and within the last three months TruSecure has recommended one patch for IIS systems, a cumulative patch that ensures all previous patches are applied) and
- Used in concert with TruSecure synergistic controls

Was completely invulnerable to both Code Red and Nimda, as well as all other known attacks within this time frame.

TruSecure believes it can be extremely easy to use IIS in a secure fashion for most requirements. TruSecure expects its customers to be cognizant of its Alerts and Monitor information, and to use the time-frame advice provided within them. TruSecure believes that its customers apply the synergistic controls, such as router access control lists, to assist in the security of even directly Internet connected IIS systems.

Further, TruSecure believes that all of the above are true for any system, whether they are Microsoft IIS or Apache on Linux. Vulnerabilities and configuration issues exist in all software, but with due diligence all can be secured for most requirements with relatively equal maintenance cost.

TruSecure

TruSecure Corporation • 13650 Dulles Technology Drive, Ste. 500. • Herndon, VA 20171-4602 • 1.888.396.8348 •
www.trusecure.com