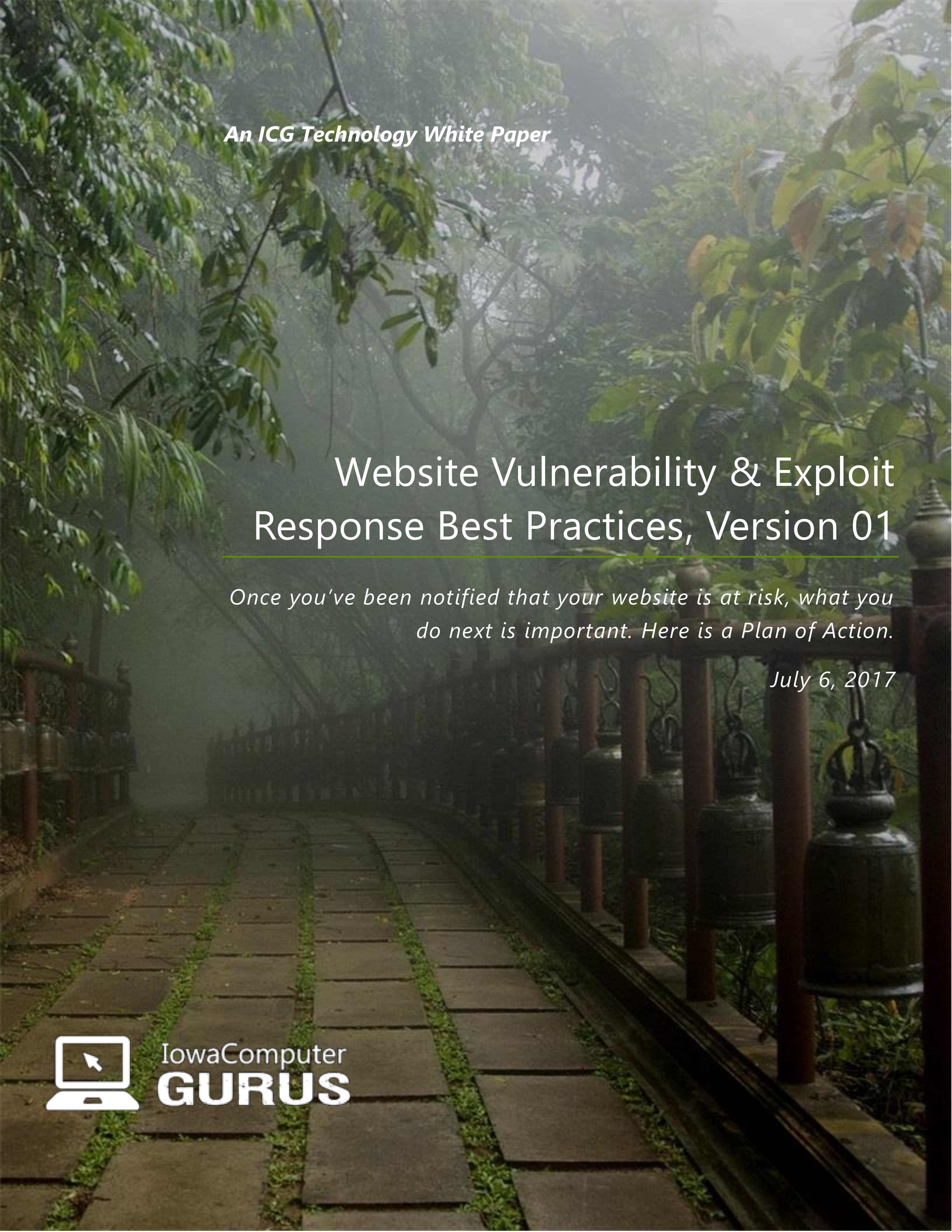


An ICG Technology White Paper

Website Vulnerability & Exploit Response Best Practices, Version 01

Once you've been notified that your website is at risk, what you do next is important. Here is a Plan of Action.

July 6, 2017

IowaComputer
GURUS

Technology Services and Support ... for the Life of Your Project

Contents

Technology Services and Support ... for the Life of Your Project

The Purpose of This Document

This document in not intended to address a targeted attack of any kind. The protocols for dealing with malicious intrusions (hacks), ransomware, or distributed denial-of-service attacks are different – although some principles may be common to those defenses.

This document was designed to help prepare for the possibility of an identified vulnerability within a modern website or application and – if such a vulnerability is discovered – provide best practices to determine a course of action that addresses issues quickly and confidently while reducing unnecessary risks and unexpected consequences. Importantly, these best practices can be implemented without regard to any particular hardware, software, application, or development platform.

Who Should Use This Document

This document is intended to be used by website developers and administrators with at least an intermediate understanding of general website design, management, development, and security principles. It may also be of value to general website owners and project managers as a tool for preparing related action plans.

Assumptions

The discussions and recommendations in this document assume the following:

- Best practices regarding data protection are established and practiced, including regular backups and backup vintage retention.
- Best practices regarding general infrastructure security are established and practiced, including scheduled firmware updates, the use of firewalls, and physical access protocols.

Document Revision History

Rev. Date	Notes
7/6/2017	First public release, Version 01.

Technology Services and Support ... for the Life of Your Project

Website Vulnerabilities and Exploits – An Overview

Website and data security is the number one issue for the internet today. When a site owner is notified that an element of their technology stack has been exposed vulnerability subject to malicious exploit, it can be difficult to know what to do to address that vulnerability safely.

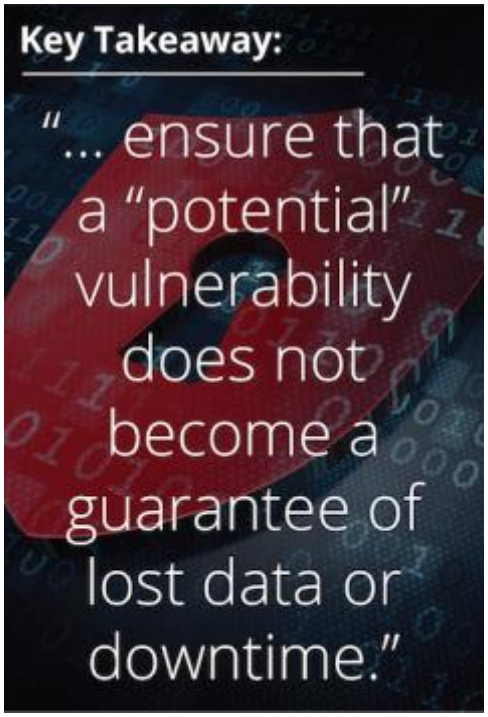
Website vulnerabilities can occur in any part of the technology stack, including:

- Content Layer
  - Media
  - Files (e.g., PDF, documents, spreadsheets)
  - Images
- Application Layer
  - Plug-ins, Add-ons, modules
  - Website Code
  - Content management System (CMS)
  - HTML
  - Database
  - Third-party analytics and security services
  - Application Framework (.NET, PHP, Java)
- Operating System (OS) Layer
  - Server Settings / Configuration
  - Webserver (e.g., Windows IIS, Apache)

There are additional potential points of vulnerability at the network and infrastructure layers, but those are outside the scope of this document.

Each of these elements can be deeply integrated with other elements, resulting in complex interactions. Since each website uses a different combination of technical elements, the number of possible derivations is nearly limitless.

So, addressing any discovered vulnerability needs to be handled deftly to ensure that a “potential” vulnerability does not become a guarantee of lost data or downtime.

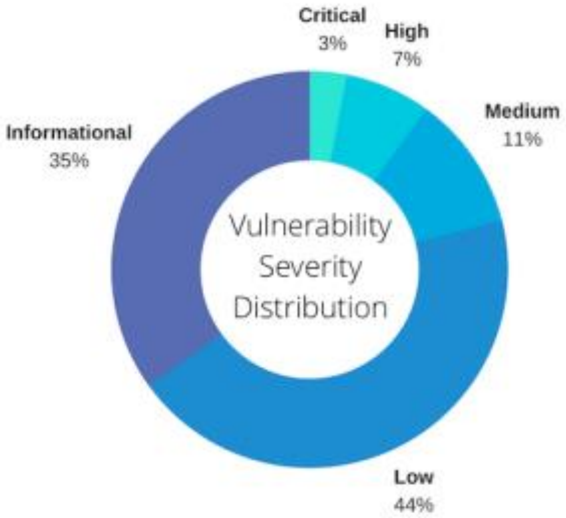

Key Takeaway:

“… ensure that a “potential” vulnerability does not become a guarantee of lost data or downtime.”

Scope, Risk, and Perspective

Recent industry reports suggest that 99.7% of all web applications have at least one known vulnerability.[1]

That's a scary statistic. But it's the "scariness" of that number can cause unnecessary reactions. The first thing to remember is that all vulnerabilities are not created equal.



The United States Computer Emergency Readiness Team (US-CERT)[2] was established in 2003 to track vulnerabilities, exploits, and other malicious cyber-activity as an impartial reference and alert authority. They classify vulnerabilities and incidents by severity:

- High Vulnerability
- Medium Vulnerability
- Low Vulnerability
- Severity Unassigned

Contrast this with Trustwave's categorization of Application Vulnerability Risk Levels:

- Critical – 3%
- High – 7%
- Medium – 11%
- Low – 44%
- Informational – 35%

All other industry-accepted, neutral sources have similar classification systems. The point is that more than three-quarters of all reported vulnerabilities are low or very low risk.

Further, a High-rated vulnerability may pose a substantial risk to some sites, and relatively little or no risk to another. Conversely, a Medium rated vulnerability can become a priority for some websites depending on their particular mix of technologies.

Key Takeaway:

> "... the discovery of a vulnerability needs to be first thoroughly assessed, then met with a response that is both proportionate to the threat and timely to the risk."

[1] 2017 Trustwave Global Security Report, June 20, 2017. Downloaded by the author on July2, 2017.

[2] More information available at: https://www.us-cert.gov

This is not to suggest that any vulnerability should remain un-addressed. It does, however, highlight that the discovery of a vulnerability needs to be first thoroughly assessed, then met with a response that is both proportionate to the threat and timely to the risk. These assessments apply to both the severity of the threat and the potential exposure of your specific systems.

Another major consideration is making the determination whether your site or web application has been compromised and the relative likelihood that it will be soon. Both of these determinations change the threat horizon.

Website Vulnerability and Exploit Response Model

In order to evaluate the risks of a vulnerability and balance the response to the level of risk, we propose the Website Vulnerability and Exploit Response model (WVER):

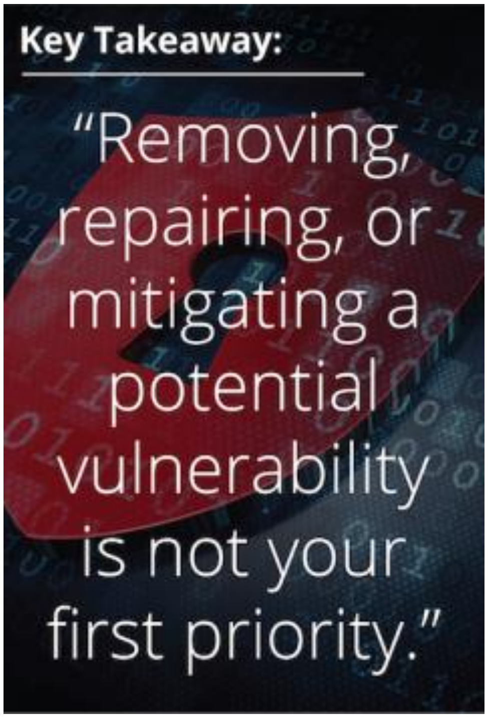
1. Notification
2. Containment
3. Analysis / Decision-making
4. Remove / Repair / Mitigate / Recover

Notification

The Notification is the triggering event for your response. Notifications can come from the technology vendor, government monitoring organizations, third-party industry sources, the media, or members of your technology team. Every potential vulnerability notification should be fully evaluated using this model.

Containment

Removing, repairing, or mitigating a potential vulnerability is not your first priority. The actions of removing, repairing, or mitigating can result in unforeseen issues of dependency or interaction. Your first priority is to protect existing data and systems., so having a rollback and recovery method in place is vital before any action is taken.



Key Takeaway:

"Removing, repairing, or mitigating a potential vulnerability is not your first priority."

[The elements of Analysis and Decision-making can be begun concurrently with Containment.]

Immediate Containment Actions

1. Confirm that the vulnerable technology is currently deployed on your systems.
2. Determine whether the vulnerability has already been exploited on your systems.
3. Run a new full backup of all systems as soon as practicable.
4. Verify and secure previous (vintage) system backups.

Technology Services and Support ... for the Life of Your Project

Analysis and Decision-making

The Analysis and Decision-making step is critical, but often misapplied or misunderstood. Since every vulnerability and system are different, the point of the analysis questions is to evaluate the potential vulnerability with regard to your specific circumstances and application.

For example, a vulnerability that exposes form field data on a page using a specific module or plug-in is of very low immediate risk if there are no forms on that page.

Another example is to consider time horizon. It is fairly common for a potential vulnerability to be identified before it has been exploited in any known live environment. If there is an active update or patch in process in such a circumstance, it may be both realistic and relevant to monitor the situation with a bias toward waiting for the update. However, if an action has recently gained public notice from the media or other sources, it may elevate in urgency.

With that in mind, the following are the elements of vulnerability Analysis and Decision-making.

Analysis

The point of Analysis is to have all the information necessary to effectively determine a course of action that considers timing, severity, and risk.

External Evaluation

- What is the severity of the vulnerability as determined by the technology provider?
- Is the technology provider working on a patch or update that mitigates or removes the vulnerability? If so, when is it expected to be released?
- What is the severity of the vulnerability as determined by US-CERT or other trusted third-party organization?

Internal Assessment

- Is the vulnerable technology relevant to your deployment?
- Is the vulnerable technology deployed to more than one location on your systems?
- Do other technology systems (e.g., modules, plugins, analytics, databases, etc.) rely on the vulnerable technology in your environment?

Risk Assessment

- How likely is the vulnerability to be exploited on your systems within the next:
  - Few hours
  - One day
  - One Week
  - Thirty Days
- Could an exploit of this vulnerability expose personally identifiable information in your application?
- Could an exploit of this vulnerability risk data corruption in your application?
- Could an exploit of this vulnerability impact control or access to systems or data in your application?
- Could an exploit of this vulnerability result in the theft of data, funds, or resources?

- Could a published vulnerability mitigation or patch impact the application functionality or user experience?

Decision-making

It is tempting to assign a numerical value to each of the analysis points listed above in order to "score" an action plan decision. But the requirements of every business and the configuration of every system is different. A medical or financial business is going to have a different threshold than a construction company, and an eCommerce site is going to have different risk profile than a marketing or brochure site.

If you have completed the analysis shown above, the next step is to gather input from all key system contributors. This should include your relevant internal technology team members and any external technology consultants and contractors (if applicable). Provide them with the analysis points and work with them to consider all potential implications before determining your recommended course of action.

Inform leadership of your intended plan and timing per your policies and procedures.

Remove, Repair, Mitigate, Recover … or Wait

Depending on the severity and risk determined by your Analysis, your action plan may fall with in a wide range of scopes and urgencies.

Key Takeaway:

> "Required actions may be immediate and significant…. sometimes the best course of action is to wait."

- Required actions may be immediate and significant, requiring an unscheduled publish out of normal maintenance windows.
- If your site or application have been compromised, the action plan may require recovering all or part of your systems from a backup performed prior to the vulnerability being exploited.
- It may require small changes with either low impact transparent to end-users and staff – such as the removal or disabling of the vulnerable asset until a more permanent solution is implemented, or following prescribed mitigation procedures provided by the technology supplier.
- In situations with lower risk, sometimes the best course of action is to wait – preparing now and then implementing corrective action at the next website publish or when the technology vendor releases an anticipated product update.

All of these courses or action are viable best practices – taken independently or in concert – depending on your thorough analysis and evaluation of your specific risks and circumstances.

IowaComputer GURUS

Custom Websites and Intranets

.NET Application Development

Expert Technology Support and Training

Performance Optimization

Technology Services and Support ... for the Life of Your Project

Summary

The first rule taught to doctors is, “do no harm.” This rule applies to managers and administrators of internet websites and applications. Each incident of a potential vulnerability needs to be independently examined and analyzed to consider the severity of the vulnerability to a particular environment, the potential risks unique to each solution, and optimal timing.

This is the only way to reasonably assure that the cure will not be more disruptive than the disease.

About IowaComputerGurus Inc.

IowaComputerGurus Inc., a Microsoft Certified Partner organization specializes in developing custom solutions using the Microsoft .NET development stack and leading Content Management Systems. Based in Des Moines, Iowa, they provide services to customers all over the world and base their business on providing quality, affordable technology solutions with the best customer service. The company is led by Mitchel Sellers, a Microsoft MVP, AP.Net Insider, Microsoft Certified Professional, DNN MVP, and published technology author.

Contacting IowaComputerGurus

IowaComputerGurus, Inc.
5550 Wild Rose Lane, Suite 400
West Des Moines, Iowa 50266

Phone: (515) 270-7063
Fax: (515) 866-591-3679
Email: webmaster@iowacomputergurus.com
Website: http://www.iowacomputergurus.com

Feedback

IowaComputerGurus is committed to quality and appreciates constructive feedback on our Best Practices documents, white papers, and other technical guides. If you discover any errors or have suggestions of additional items for inclusion or any modifications to existing content, please use one of the above listed contact methods to let us know.

Disclaimer

This document reflects the opinions and experience of the authors as a non-compensated service to the community. It is provided “as-is,” and no warrantee is expressed or implied as to the serviceability or applicability of any information or recommendation for any particular purpose, application, and / or environment. It is the reader’s responsibility to conduct their own diligent research, consult experts, and determine whether this information is right for their website, application, and / or environment. Additionally, the reader understands that the use of this documentation constitutes agreement to the any additional relevant terms of use as currently published on the IowaComputerGurus.com website, which are subject to change.

Copyright and Trademark Notices