



**Media Contacts:**

Patricia Koebele

Digital Defense, Inc.

210.582.6128

[patricia.koebele@ddifrontline.com](mailto:patricia.koebele@ddifrontline.com)

**DIGITAL DEFENSE RELEASES CRITICAL DNS VULNERABILITY CHECK**

**San Antonio, TX – August 4, 2008** –[Digital Defense, Inc.](#) (DDI), a leading provider of information security assessment services and Security Information and Assessment Management (SIAM) solutions, announced they recently implemented an important DNS (Domain Name System) consolidated vulnerability check within their Frontline Vulnerability Scanner. The new vulnerability check is associated with the recently disclosed multi-vendor [DNS cache-poisoning vulnerability](#) and DDI has already released it to their client base.

“Our Vulnerability Research Team (VRT) immediately realized the gravity of this vulnerability and developed a unique, non-banner based detection method to address the issue. Because of our remote scanning ability and Software as a Service (SaaS) approach to fulfillment, we are able to detect the presence of this critical vulnerability with specially crafted DNS queries to test both external and internal DNS servers, regardless of the software vendor,” said [Gordon MacKay](#), Vice President of Vulnerability Research & Platform Development at Digital Defense. “Security is a continual process and our VRT and Security Operations Team strive on a daily basis to proactively detect, test, track, and report on the vulnerabilities that impact our clients. Our ability to immediately address this DNS vulnerability is evidence of that fact.”

DDI’s [proprietary assessment engine](#), combined with the Company’s [Frontline™ Vulnerability Lifecycle Management](#) offering, provides enterprise-wide, distributed network scanning capabilities on an on-demand basis. Via the offering, clients can assess any device within their network on an on-demand basis, regardless of its geographic location. Additionally, clients can also avail themselves to the Frontline portal, which DDI architected to best support the needs of each client in terms of scan and penetration test reporting and workflow management. Via additional modules contained within the Frontline portal, clients can also associate business risk with each device, allowing for further optimization of their risk mitigation plans. Simply put, DDI clients subscribing to the Vulnerability Lifecycle Management and [Penetration Test](#) services benefit not only from DDI’s ongoing investment in their SaaS platform and solutions, but the strength and integrity of their [VRT](#) and [Security Operations Teams](#) as well.

**About Digital Defense**

Digital Defense, Inc. (DDI), a Payment Card Industry Security Standards Council approved scanning vendor, delivers a comprehensive portfolio of risk management services including information security programs, regulatory compliance solutions, security testing of IT products and security education offerings. DDI and its Security Operations team uses proprietary Software as a Service (SaaS) technology and industry best practices to deliver a broad array of services to clients, which range from small financial institutions to global Fortune enterprises. Frontline™, DDI's flagship service portal, provides clients with instant access to a SIAM platform that enables independent oversight of their organization's security posture on an autonomous or DDI-managed service basis. In addition to headquarters in San Antonio, DDI maintains offices in Austin, and Houston, TX, Colorado Springs, CO, Greenville, SC, Milwaukee, WI and Kihei on Maui, HI. For more information about Digital Defense, please visit our web site at [www.ddifrontline.com](http://www.ddifrontline.com) or contact us at 888.273.1412.

### **Reader Contact Information**

Digital Defense, Inc., 9000 Tesoro Drive, Suite 100, San Antonio, Texas, 78217

Phone - 210.822.2645, Fax - 210.822.9216

[www.ddifrontline.com](http://www.ddifrontline.com)

###

Digital Defense and the Shield Logo are Registered Service Marks of Digital Defense, Inc. All other trademarks are the property of their respective owners.