

AFFIDAVIT OF NATHANIEL E FRANK-WHITE

1. I am a Records Request Processor at the Internet Archive. I make this declaration of my own personal knowledge.
2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.
3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to browse more than 450 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a display of available dates. The visitor may select one of those dates, and begin browsing an archived version of the Web. Links on archived files in the Wayback Machine point to other archived files (whether HTML pages or other file types), if any are found for the URL indicated by a given link. For instance, the Wayback Machine is designed such that when a visitor clicks on a hyperlink on an archived page that points to another URL, the visitor will be served the archived file found for the hyperlink's URL with the closest available date to the initial file containing the hyperlink.
4. The archived data made viewable and browsable by the Wayback Machine is obtained by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.
5. The Internet Archive assigns a URL on its site to the archived files in the format `http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL]` aka an "extended URL". Thus, the extended URL `http://web.archive.org/web/19970126045828/http://www.archive.org/` would be the URL for the record of the Internet Archive home page HTML file (`http://www.archive.org/`) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). The date indicated by an extended URL applies to a preserved instance of a file for a given URL, but not necessarily to any other files linked therein. Thus, in the case of a page constituted by a primary HTML file and other separate files (e.g., files with images, audio, multimedia, design elements, or other embedded content) linked within that primary HTML file, the primary HTML file and the other files will each have their own respective extended URLs and may not have been archived on the same dates.
6. Attached hereto as Exhibit A are true and accurate copies of screenshots of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached coversheet of each printout.



7. I declare under penalty of perjury that the foregoing is true and correct.

DATE: 12/08/2022

Please see attached
All Purpose
Jurat form
for additional
Notary Events

Nathaniel Frank-White
Nathaniel E Frank-White



EXHIBIT A





http://www.assurent.com/index.php?id=58

Go

OCT

FEB

APR

02

2006

2007

2008

About this capture

15 captures

10 Feb 2006 - 30 Apr 2009

15 captures

10 Feb 2006 - 30 Apr 2009

HOME

COMPANY

SOLUTIONS

SERVICES

RESEARCH

PRODUCTS

assurent

secure technologies

a TELUS Company

contact us

search

Products

Home > Products > Vulnerability Data

Web Application Firewall

Secure Software Development Model

Vulnerability Data

Spyware Data

Vulnerability Data

Assurent's Vulnerability Research Services provide a range of services focused on security vulnerability research and engineering. Our offerings provide both the industry's best response time for early warning of emerging threats, and in-depth, lab-based analysis of vulnerabilities based on disassembly, protocol analysis, and source analysis. Our vulnerability data enables security product vendors to deliver product updates (signatures, filters, scripts) without the need for additional research, and empowers MSPs and enterprise security teams with tools and knowledge to more effectively protect their environments.

Assurent delivers detailed, factual content to our subscribers that includes:

- ▶ The industry's best response time for early warning of emerging threats
- ▶ Complete information regarding the internal technical mechanism of vulnerabilities and threats
- ▶ Details for both network-based and host-based detection of any possible attack attempting to exploit a vulnerability
- ▶ Details for accurate network-based and host-based differentiation between systems that are vulnerable and those that are not
- ▶ Sample exploit code authored by Assurent
- ▶ Packet captures of both baseline traffic and attack cases
- ▶ Full cross-references to vendor advisories, CVE, and third-party databases

A dedicated team of experienced information security professionals focused exclusively on security vulnerability engineering delivers these services. Team members validate and reproduce reported security vulnerabilities (supporting all major operating systems, platforms, and enterprise products), develop detection signatures and filters for network-based and host-based IDS and IPS systems, create probes and scripts for vulnerability assessment tools, and develop custom security tools. In addition, the VR Team performs original research on a contract basis.

Assurent's principal Vulnerability Research offerings include: Vulnerability Research Subscription feeds for security product vendors, for managed service providers, and for enterprise security teams, which provide near real-time coverage for the most severe security vulnerabilities in software products and networking devices, and the Vulnerability Research Database, containing detailed information on historical vulnerabilities.

Assurent's vulnerability research offerings include:

- [Vulnerability Research for Security Product Vendors](#)
- [Threat Protection Program for Managed Service Providers](#)
- [Threat Protection Program for Enterprise Security Teams](#)
- [Spyware Data](#)
- [VR Portal](#)
- [VR Trials and Sample Reports](#)

Related Assurent products include:

- [Assurent Web Application Firewall](#)

© 2005 Assurent Secure Technologies. All rights reserved.

legal notice · privacy



JURAT ATTACHMENT

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF Texas }

COUNTY OF Harris }

The foregoing instrument was subscribed and sworn before me this date of
12/08/2022, by Nathaniel Frank-White

This notarial act was an online notarization.



(Notary Seal)

Notary's Signature Ana Laura Salazar Uribe

Registration No.: 131757026

Commission Expiration Date: October 11, 2026

