FOR OFFICIAL USE ONLY

# Certificate of Networthiness (CoN)

**Product:** Vulnerator 6.x

| Cert# | Request Type | CoN Type | Approval | Expiration |
|---|---|---|---|---|
| 201620794 | Modify | Enterprise | 4/18/2016 | 4/18/2019 |
| **Mission Area** | **Domain** | **Functional Area** | **Category** | |
| Enterprise Infrastructure Environment | IA | Security | Application | |

**Description:**

Vulnerator 6.x is a Government developed application by the Defense Information Systems Agency (DISA) to support the Forge.mil program. Forge.mil enables the collaborative development and use of open source and DoD community source software in support of the Net-centric operations and warfare. Vulnerator is a C#/.Net application that imports and aggregates finding data from the DoD Gold Disk, Unix SRR, eEye Retina Security Scanner, eEye Retina Security Content Automation Protocol (SCAP) Scanner, Navy Windows Automated Security Scanning Program (WASSP), SPAWAR SCAP Compliance Checker, and DISA Security Technical Implementation Guides (STIG) Viewer. A detailed report is generated in an XML format that is opened with Microsoft Excel. This tool contains multiple tabs that report many different statistics. Included in the report is Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) and a formatted Plan of Action and Milestones (POA&M).

Vulnerator 6.x is installed on a current AGM build workstation. CAC authenticated users execute the application from the shortcut in the Windows Start menu or from the desktop icon. The user is prompted to enter configuration information as well as point to input files of scan data. Once the configuration is completed, the application creates a comma-separated values file readable by Microsoft Excel. This file contains multiple tabs including hardware listing, software listing, vulnerability detail, and a DIACAP standard POA&M. The resulting comma-separated values file is saved to the workstation. Data stays internal to the local enclave.

**Facts:**

- This is a modification for Certificate 201620785.
- This product is an Open Source Software (OSS).

**CoN Link:** https://portal.netcom.army.mil/apps/networthiness/_layouts/NetcomCON/rqstcon2.aspx?requestId=30878

**Restrictions:**

1. The organization implementing this open source software will ensure the source code is available for examination; applicable configuration implementation guidance is available, a protection profile is in place, or a risk and vulnerability assessment has been conducted with mitigation strategies implemented. This capability requires CCB approval and documentation prior to implementation. Notification of the supporting Regional Cyber Center (RCC) of local software use approval is required.
2. Vulnerator 6.x is restricted for use within certified and accredited networks and/or data centers having a current ATO.

**POC:** netcom.hq.networthiness@mail.mil /(520)538-1199

This Certificate of Networthiness is based on a trusted standardized platform, configured per FDCC. All patches and updates will be provided by the host network administrator (NEC or DECC) in accordance with all technical directives, mandates, and IAVM. This Certificate of Networthiness is no longer valid should the assessed configuration be significantly altered. Per Army Cyber Command guidance, all operating environment will implement HBSS capabilities. Upon expiration of this Certificate of Networthiness, this application must be reassessed to ensure it is still compliant with the GNEC architecture and is still networthy. Should this software version be upgraded prior to this expiration, the new version must be evaluated for networthiness.

**Additional Comments:**

X BRADFORD.DANIEL.1124817257
Signed on 2016-04-18T04:00:00Z

Daniel Q. Bradford
Senior Executive Service (SES), Deputy to the Commander / Senior Technical Director / Chief Engineer
Network Enterprise Technology Command (NETCOM)