CISA CYBERSECURITY DIRECTIVE 21-02

Actions Required to Respond to Microsoft Exchange Server Vulnerabilities

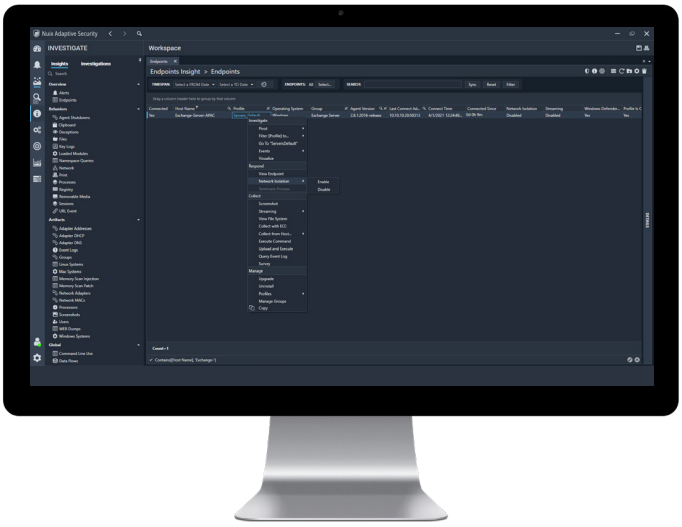
The Cybersecurity and Infrastructure Security Agency issued Emergency Directive 21-02 on March 3, 2021. Titled *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, the directive details vulnerabilities in Microsoft Exchange Server products that attackers could use to gain access to systems or networks running these products.

Using components of the Nuix software platform, agencies can quickly identify, mitigate and remediate attacks made using these vulnerabilities.

RAPID TRIAGE AND RESPONSE

Nuix Workstation connects directly to Exchange Servers and most other network servers and repositories as well as the system files and logs. This enables forensic triage but eliminates the time wasted to acquire a forensic image of the Exchange Server to perform early case assessment or triage the system.

The Nuix Workstation YARA, IOC and RegRipper scripts automate the process of identifying indicators of compromise, getting answers within minutes of the Exchange Server examination. Nuix Adaptive Security will proactively alert agency staff to indicators of compromise or anomalous behavior, such as credential dumping, lateral movement, persistence mechanisms and other follow-on exploitation activity on the Exchange Server.

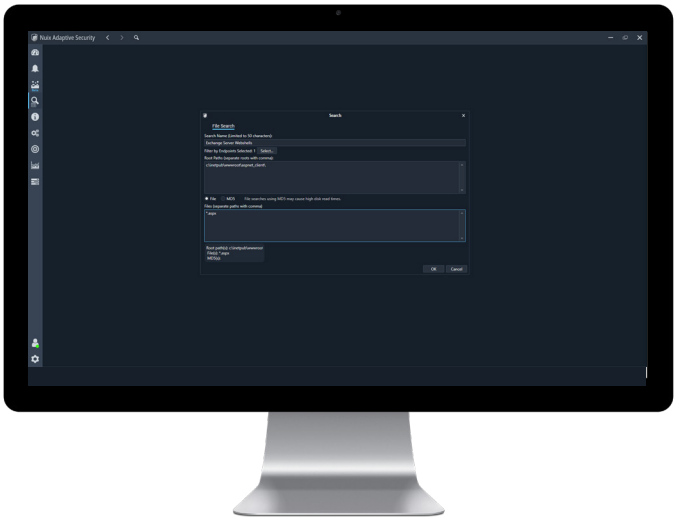


Temporarily isolate the potentially compromised Microsoft Exchange server directly from Nuix Adaptive Security.

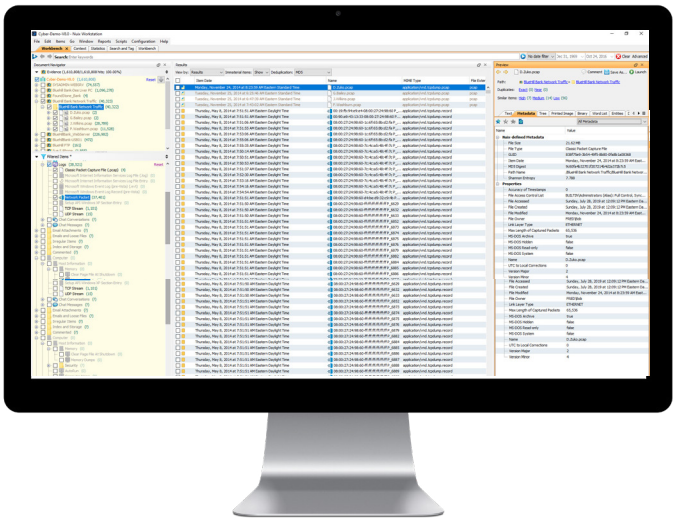
POWERFUL REMEDIATION

Nuix enables all the functional requirements identified in this Emergency Directive and likely the requirements of future Emergency Directives. Additionally, Nuix Enterprise Collection Center provides agency staff with integrated workflows to quickly remediate indicators of compromise on Exchange Servers and other endpoints on the network.

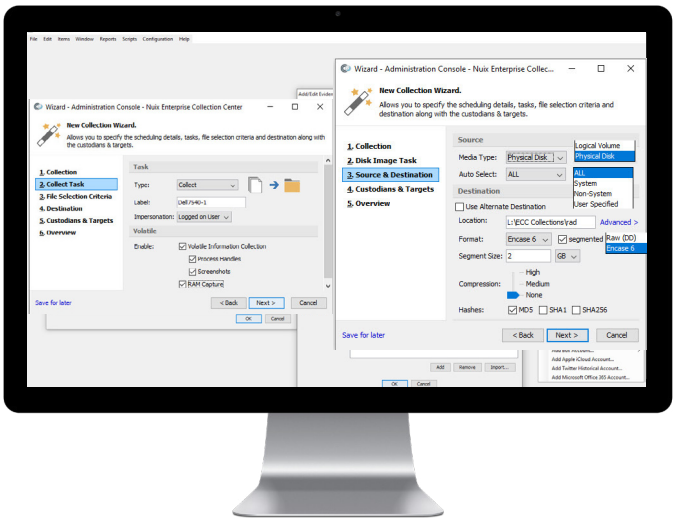
In addition, Nuix Adaptive Security lets agency staff isolate the Exchange Server or endpoints to prevent lateral migration of malware.



Using Nuix Adaptive Security, you can search for indicators of compromise, including the web shells identified in CISA's alert, as well as collect and delete files on the endpoint.



Nuix Workstation provides unparalleled visibility into the details of network activity pulled from endpoints.



Nuix Enterprise Collection Center provides additional enterprise collection and deletion features, including full disk imaging.

RAPID, DEFENSIBLE RESULTS AT ENTERPRISE SCALE

While open source tools are useful, Nuix provides a fully supported defensible forensic solution with real-time enterprise-wide visibility required to respond to CISA's guidance and defend against advanced attacks in the future. Nuix is backed by decades of forensic, cybersecurity and incident response expertise to provide an integrated threat mitigation and remediation solution trusted by organizations globally.

Nuix (www.nuix.com, ASX:NXL) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849