



Results in Brief

OIG 19-10
May 1, 2019

Audit of WMATA's End-of-Service Life Operating System Software

Why We Did This Review

While conducting the Audit of WMATA's *Security Over Publicly Accessible Web Applications*, OIG 19-02, the Office of Inspector General (OIG) found WMATA has systems with end-of-life and end-of-support Microsoft operating systems. As such the OIG decided to conduct an Audit of WMATA's Software Asset Management Program. This report is the first report on WMATA's management of its software assets.

Microsoft provides: “[e]very Windows product has a lifecycle. The lifecycle begins when a product is released and ends when it's no longer supported. Knowing key dates in this lifecycle helps you make informed decisions about when to update, upgrade or make other changes to your software.”

The WannaCry and Petya viruses are ransomware that exploited vulnerabilities in operating systems. The exploit attacks were worldwide and required system owners to pay a ransom in bitcoins to regain access to their respective systems. The attacks cost organizations millions of dollars and impaired operations.

The objective of this audit is to assess WMATA's management of software reaching or that has reached the end of its service life (EOSL).

What We Found

WMATA had operating systems and contractor-owned systems that were running end-of-service life operating system (O/S) software. The end of vendor support for the various O/S software had, in some cases, ended years earlier.

When vendors stop supporting older versions of their products, those products pose significant security risks because updates are no longer available. These vulnerabilities increase the opportunities for cyberattack, data breaches, and vulnerability exploits. If left unaddressed and thereafter exploited, these vulnerabilities could have monetary impacts, impair operations, endanger public safety, and damage WMATA's reputation. Further, EOSL O/S software may: (1) prevent WMATA from using more current, effective, and efficient devices and solutions; (2) decrease productivity; (3) increase maintenance costs; and (4) decrease reliability.

Management's Response

WMATA's Executive Vice President, Internal Business Operations, and Executive Vice President and Chief Operating Officer provided written comments dated April 11, 2019, in which they concurred with the finding and recommendations. OIG considers management's comments responsive to the recommendations and corrective actions taken or planned should correct the deficiencies identified in the report.

NOTE

THIS REPORT CONTAINS SECURITY-RELATED INFORMATION AND IS NOT PUBLICLY AVAILABLE