Homeland Security Warns of Oracle, SAP Vulnerabilities

Written by Marco Attard
27 July 2018

The Department of Homeland Security issues an alert of potential vulnerabilities in Oracle and SAP enterprise resource planning (ERP) software, following a report from security firms Onapsis and Digital Shadows.

The security firms state firms in the UK, US and Germany are at most risk from the threat-- and warn state-sponsored actors and hacktivists groups are targeting ERP applications used by large businesses to steal sensitive data, such as financial results, manufacturing secrets and credit card numbers. In fact, systems at two government agencies and media, energy and finance firms have already been hit, following failure to install patches and take other security measures.

The "ERP Application Under Fire" report lists over 200 SAP and 2500 Oracle exploits, some dating back over a decade. For instance, several botnets of the Dridex malware, set up over 2017 and 2018, allow cyber criminals to steal valid SAP user credentials for access into internal IT environments. Another exploit dates back to 2013, with the Sudoh@ck3rs attack of an internet-facing SAP portal.

"While some executives still consider 'behind-the-firewall' ERP implementations to be protected, we have observed clear indicators of malicious activity targeting environments without direct internet connectivity," the report reads. "Further, there is an astonishing number of insecure ERP applications directly accessible online, both on-premise and in public cloud environments, increasing the attack surface and exposure."

In turn, both Oracle and SAP state the vulnerabilities have been patched out, but customers refuse to apply them due to fear of disruption to manufacturing, sales or finance activities. Also leading to further risk are installation mistakes or growing moves to link traditional back-office systems to the cloud.

As for a solution, the security firms suggest identifying ERP application layer vulnerabilities, monitoring for leaked ERP data and user credentials, and identifying and removing any dangerous interfaces and APIs between the different ERP applications in an organisation.

Go ERP Applications Under Fire