Talos Vulnerability Report

TALOS-2020-1147

Kepware LinkMaster Service privilege escalation vulnerability

DECEMBER 16, 2020

CVE NUMBER

CVE-2020-13535

Summary

A privilege escalation vulnerability exists in Kepware LinkMaster 3.0.94.0. In its default configuration, an attacker can globally overwrite service configuration to execute arbitrary code with NT SYSTEM privileges.

Tested Versions

Kepware LinkMaster 3.0.94.0

Product URLs

https://www.kepware.com/en-us/products/linkmaster/

CVSSv3 Score

9.3 - CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-276 - Incorrect Default Permissions

Details

Kepware LinkMaster is a product linking various OPC servers and clients providing a means of communication between current DDE/OPC and legacy clients and applications.

The vulnerability arises due to incorrect defauly permissions set on LinkMasterV3 service which grants Everyone group access to the `SERVICE_CHANGE_CONFIG` option allowing anyone to reconfigurethe service in any manner. A local attacker can use this vulnerability to modify the existing service binary to point to an arbitrary executable which will run with `NT SYSTEM` privileges.

```
LinkMasterV3
  RW Everyone
                SERVICE_QUERY_STATUS
                SERVICE_QUERY_CONFIG
                SERVICE_CHANGE_CONFIG
                SERVICE_START
                SERVICE_STOP
  RW NT AUTHORITY\SYSTEM
                SERVICE_ALL_ACCESS
  RW BUILTIN\Administrators
                SERVICE_ALL_ACCESS
```

Timeline

2020-09-08 - Vendor Disclosure
2020-12-16 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2020-1136

NEXT REPORT

TALOS-2020-1150