DupScout Enterprise 10.0.18 BoF

Summary

Name	DupScout Enterprise 10.0.18 'sid' Buffer Overflow

Fixed versions	13.2.24
Release date	2020-12-15 14:00 COT

Vulnerability

Kind	Stack Buffer Overflow
Rule	345. Establish protections against overflows
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSSv3 Base Score	9.8 CRITICAL
CVSSv2 Vector	AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSSv2 Base Score	10 HIGH
Exploit available	Yes
Exploit URL	https://www.exploit-db.com/exploits/49217
CVE ID(s)	CVE-2020-29659

Description

A stack buffer overflow was found in the `sid GET` parameter of several requests of DupScout Enterprise 10.0.18 which can be exploited by an unauthenticated, remote user to gain `NT AUTHORITY\SYSTEM` privileges on the server holding the affected software.

Exploit

A first version of the exploit was published at Exploit DB and an updated exploit can be found here.

Mitigation

An updated version of DupScout Enterprise is available at the vendor page.

Credits

The vulnerability was discovered by Andrés Roldán from the Offensive Team of `Fluid Attacks.`

References

CVE https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29659

Exploit https://www.exploit-db.com/exploits/49217

Updated exploit prine-exploit.py

Vendor page https://www.dupscout.com/