Oce Colorwave 500 printer - multiple vulnerabilities

From: Red Timmy Security <publications () redtimmy com>
Date: Thu, 19 Mar 2020 17:53:44 +0100

Hi,
we have recently registered five CVE(s) affecting the Oce Colorwave 500 printer.

CVE-2020-10669 is an authentication bypass allowing an attacker to access documents that have been uploaded to the printer. As the documents remain stored in the system even after they have been printed (depending on the printer's configuration), a malicious insider may be able to access documents printed in the past.

CVE-2020-10667 is a Stored XSS on the "/TemplateManager/indexExternalLocation.jsp" page.

CVE-2020-10668 and CVE-10670 are two Reflected XSS on pages "/home.jsp" and "/SettingsEditor/settingDialogContent.jsp".

Finally CVE-10671 is a system-wide CSRF due to the absence of any form of nonce or countermeasure protecting against Cross Site Request Forgery.

More details and full story here: https://www.redtimmy.com/red-teaming/hacking-the-oce-colorwave-printer-when-a-quick-security-assessment-determines-the-success-of-a-red-team-exercise/

regards

____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

By Date By Thread

Current thread:

- **RichFaces exploitation toolkit** *Red Timmy Security (Mar 13)*
  - **Oce Colorwave 500 printer - multiple vulnerabilities** *Red Timmy Security (Mar 20)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License