



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits de Cisco
Numéro de Référence	40620303/23
Date de publication	03 Mars 2023
Risque	Important
Impact	Critique

Systemes affectés

- Cisco IP Phone 6800, 7800, 7900, and 8800 Series
- Cisco Unified Intelligence Center
- Cisco Webex App for Web Cross-Site Scripting
- Cisco Finesse Reverse Proxy
- Cisco Prime Infrastructure and Evolved Programmable Network Manager

Identificateurs externes

CVE-2023-20078 CVE-2023-20079 CVE-2023-20061 CVE-2023-20062
CVE-2023-20088 CVE-2023-20069

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du contenu dans une page ou de causer un déni de service.

Solution

Veillez se référer aux bulletins de sécurité de Cisco pour mettre à jours vos équipements.

Risques

- Injection de contenu dans une page
- Déni de service

Références

Bulletins de sécurité de Cisco :

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-Yn8HHsMJ>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-proxy-dos-vY5dQhrV>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-epnm-xss-mZShH2J>