



BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans les produits Broadcom
<b>Numéro de Référence</b>	50520511/24
<b>Date de Publication</b>	05 Novembre 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

Systemes affectés

- ASG-S200 version 7.3.x antérieure à 7.3.23.1
- ASG-S200 version 7.4.x antérieure à 7.4.7.1
- ASG-S400 version 7.3.x antérieure à 7.3.23.1
- ASG-S400 version 7.4.x antérieure à 7.4.7.1
- ASG-S500 version 7.3.x antérieure à 7.3.23.1
- ASG-S500 version 7.4.x antérieure à 7.4.7.1
- CAS-S200 version 7.3.x antérieure à 7.3.23.1
- CAS-S200 version 7.4.x antérieure à 7.4.7.1
- CAS-S200-A1 version 7.3.x antérieure à 7.3.23.1
- CAS-S200-A1 version 7.4.x antérieure à 7.4.7.1
- CAS-S400 version 7.3.x antérieure à 7.3.23.1
- CAS-S400 version 7.4.x antérieure à 7.4.7.1
- CAS-S500 version 7.3.x antérieure à 7.3.23.1
- CAS-S500 version 7.4.x antérieure à 7.4.7.1
- Content Analysis Software version 7.3.x antérieure à 7.3.23.1
- Content Analysis Software version 7.4.x antérieure à 7.4.7.1
- ISG Content Analysis version 7.4.x antérieure à 7.4.7.1
- ISG Content Analysis version 7.3.x antérieure à 7.3.23.1
- ISG Proxy version 7.4.x antérieure à 7.4.7.1
- ISG Proxy version 7.3.x antérieure à 7.3.23.1
- Management Center - VA version 7.3.x antérieure à 7.3.23.1

- Management Center - VA version 7.4.x antérieure à 7.4.7.1
- Management Center version 7.3.x antérieure à 7.3.23.1
- Management Center version 7.4.x antérieure à 7.4.7.1
- MC-S400-20 version 7.3.x antérieure à 7.3.23.1
- MC-S400-20 version 7.4.x antérieure à 7.4.7.1
- ProxySG Software - SGOS version 7.3.x antérieure à 7.3.23.1
- ProxySG Software - SGOS version 7.4.x antérieure à 7.4.7.1
- Reporter version 7.3.x antérieure à 7.3.23.1
- Reporter version 7.4.x antérieure à 7.4.7.1
- Reporter-S500 version 7.3.x antérieure à 7.3.23.1
- Reporter-S500 version 7.4.x antérieure à 7.4.7.1
- Reporter-VA version 7.3.x antérieure à 7.3.23.1
- Reporter-VA version 7.4.x antérieure à 7.4.7.1
- SG-S200 version 7.3.x antérieure à 7.3.23.1
- SG-S200 version 7.4.x antérieure à 7.4.7.1
- SG-S200-40 version 7.3.x antérieure à 7.3.23.1
- SG-S200-40 version 7.4.x antérieure à 7.4.7.1
- SG-S200-RP version 7.3.x antérieure à 7.3.23.1
- SG-S200-RP version 7.4.x antérieure à 7.4.7.1
- SG-S400 version 7.3.x antérieure à 7.3.23.1
- SG-S400 version 7.4.x antérieure à 7.4.7.1
- SG-S400-RP version 7.3.x antérieure à 7.3.23.1
- SG-S400-RP version 7.4.x antérieure à 7.4.7.1
- SG-S500 version 7.3.x antérieure à 7.3.23.1
- SG-S500 version 7.4.x antérieure à 7.4.7.1
- SG-S500-RP version 7.3.x antérieure à 7.3.23.1
- SG-S500-RP version 7.4.x antérieure à 7.4.7.1
- SSL Visibility Appliance Software version 7.3.x antérieure à 7.3.23.1
- SSL Visibility Appliance Software version 7.4.x antérieure à 7.4.7.1
- SSP version 7.3.x antérieure à 7.3.23.1
- SSP version 7.4.x antérieure à 7.4.7.1
- SSP-S210 PLATFORM version 7.3.x antérieure à 7.3.23.1
- SSP-S210 PLATFORM version 7.4.x antérieure à 7.4.7.1

- SSP-S410 PLATFORM version 7.3.x antérieure à 7.3.23.1
- SSP-S410 PLATFORM version 7.4.x antérieure à 7.4.7.1
- SSP-S410 version 7.3.x antérieure à 7.3.23.1
- SSP-S410 version 7.4.x antérieure à 7.4.7.1
- SV-1800 version 7.3.x antérieure à 7.3.23.1
- SV-1800 version 7.4.x antérieure à 7.4.7.1
- SV-2800 version 7.3.x antérieure à 7.3.23.1
- SV-2800 version 7.4.x antérieure à 7.4.7.1
- SV-3800 version 7.3.x antérieure à 7.3.23.1
- SV-3800 version 7.4.x antérieure à 7.4.7.1
- SV-550 version 7.3.x antérieure à 7.3.23.1
- SV-550 version 7.4.x antérieure à 7.4.7.1
- SV-800 version 7.3.x antérieure à 7.3.23.1
- SV-800 version 7.4.x antérieure à 7.4.7.1

### Identificateurs externes

- CVE-2024-3596

### Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans les produits Broadcom susmentionnés. Une exploitation réussie de cette faille pourrait permettre à un attaquant de contourner la politique de sécurité.

### Solution :

Veillez se référer au bulletin de sécurité Broadcom du 01 novembre 2024 pour plus d'information.

### Risque :

- Contournement de la politique de sécurité

### Annexe

Bulletin de sécurité Broadcom du 01 novembre 2024:

- <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25157>