# D-Link تنشر إجراءات تخفيف لثغرات غير مصحّحة في مبدّلات DGS-3130



نشرت D-Link إجراءات تخفيف لعدة ثغرات أمنية غير مصحّحة في مبدّلات DGS-3130 المُدارة القابلة للتكديس. على المشغّلين مراجعة إرشادات الشركة.

- نشرت D-Link إجراءات تخفيف خاصة بسلسلة DGS-3130.
- المنتجات المتأثرة هي مبدّلات Gigabit مُدارة وقابلة للتكديس.
- الثغرات متعددة وغير مصحّحة، ولذلك يبقى التخفيف هو الإجراء المتاح.
- المقتطف المتاح لا يذكر أرقام CVE أو تفاصيل فنية أو مواعيد للتحديثات.

## ما الذي أُعلن

نشرت D-Link إجراءات تخفيف لعدة ثغرات أمنية تؤثر في سلسلة DGS-3130 من مبدّلات Gigabit المُدارة القابلة

للتكديس. وبحسب التقرير، لا تتوافر حتى الآن تصحيحات لهذه الثغرات، ولذلك توجّه الشركة عملاءها إلى إجراءات مؤقتة.

## ما الذي لم يتضح بعد

لا يتضمن المقتطف المتاح لنا أرقام CVE ولا طبيعة الثغرات الفنية ولا إصدارات البرنامج الثابت المتأثرة ولا موعدًا للإصلاح. لذا لا نستنتج شيئًا عن الخطورة أو الاستغلال يتجاوز ما ذكرته الشركة، وينبغي للفرق الرجوع إلى إرشادات المورّد الأصلية قبل اتخاذ أي إجراء.

## الخطوات المقترحة

على المؤسسات التي تستخدم هذه المبدّلات في الفروع أو مراكز البيانات أو الشبكات الداخلية أن تتحقق أولاً من وجود أجهزة DGS-3130، بما في ذلك الأجهزة المكدّسة والمواقع الأقل ظهورًا. وبعد حصرها، تُطبَّق إجراءات التخفيف الصادرة عن المورّد ويُقيَّد الوصول إلى واجهات إدارة هذه الأجهزة. كما يُنصح بمتابعة صفحة التنبيهات لدى المورّد لمعرفة تحديثات البرنامج الثابت، وتجهيز نافذة تغيير تتيح تطبيق التصحيح بسرعة عند صدوره.

وإذا كانت الأجهزة تدعم خدمات حرجة، يُسجَّل التعرض في سجل المخاطر مع تحديد مسؤول وموعد مراجعة إلى حين تثبيت الإصلاح.

## ما يجب فعله الآن

1. حصر جميع مبدّلات سلسلة DGS-3130 بما فيها الوحدات المكدّسة والمواقع البعيدة.
2. قراءة إرشادات التخفيف من المورّد وتطبيقها على كل مبدّل متأثر.
3. حصر الوصول إلى واجهات إدارة المبدّلات في شبكة إدارة مخصصة أو أجهزة محددة بالاسم.
4. متابعة صفحة تنبيهات D-Link وتجهيز نافذة تغيير لتحديثات البرنامج الثابت عند صدورها.
5. تسجيل التعرض غير المصحّح في سجل المخاطر مع تحديد مسؤول وموعد مراجعة.