Consumer Rights Wiki

Search Consumer Rights Wiki Search Create account Log in

3CX

Page Discussion Read Edit Edit source View history Tools

❗ Article Status Notice: This Article is a stub

This article is underdeveloped, and needs additional work to meet the wiki's Content Guidelines and be in line with our Mission Statement for comprehensive coverage of consumer protection issues.

Learn more ▼

3CX, Inc., is a software development company and developer of the 3CX Phone System[1] founded in Cyprus in 2005-11-01.

The 3CX Phone System is a digital private branch exchange based on the Session Initiation Protocol (SIP) standard facilitating calls via either the public switched telephone network (PSTN) or using Voice over Internet Protocol (VoIP) services [1].

In 2023, during a major supply chain attack affecting the 3CX desktop application, the company's public response included engaging the services of Google-owned cybersecurity firm Mandiant[2] and advising customers to uninstall affected versions.

3CX

Basic information

Founded	2005-11-01
Legal Structure	Private
Industry	Telecommunication
Official website	https://www.3cx.com/

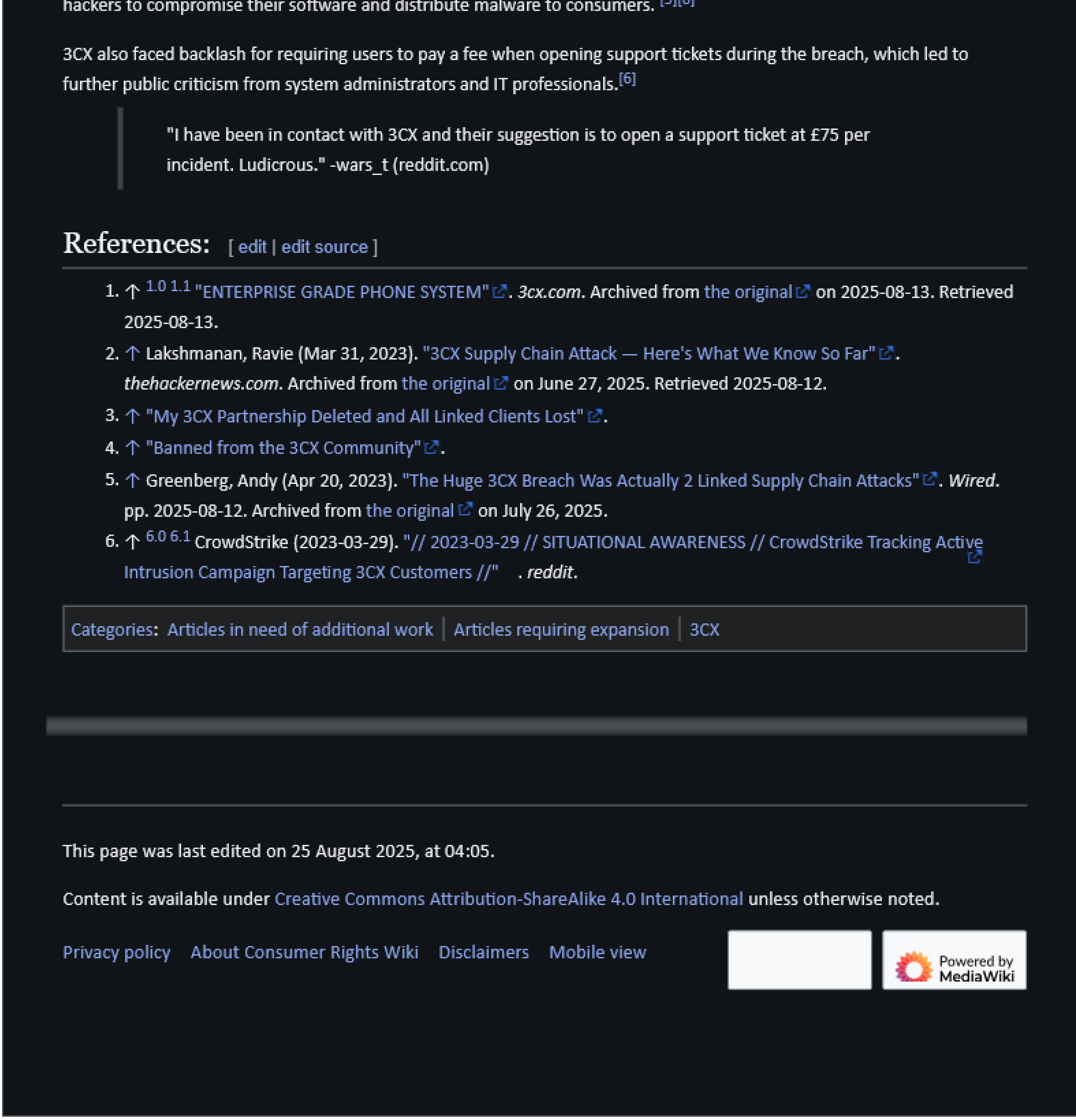
Controversies [edit | edit source]

Customer and Partner Relations [edit | edit source]

The company's CTO, Nick Galea, has been the subject of criticism from some 3CX users and partners for alleged heavy-handed moderation practices and perceived unprofessional conduct in public forums. Multiple users on Reddit have reported being banned from the official 3CX community forums for raising technical concerns or criticizing company policies. [3][4]

Supply Chain Incident Response [edit | edit source]

In March 2023, 3CX was the victim of a high-profile supply chain hack, thought to be the result of a cascade failure starting with the software X_Trader. This attack was linked to an earlier incident perpetrated by North Korean hackers, targeting software company Trading Technologies. A 3CX employee's PC containing the Trading Technologies App was used by the



hackers to compromise their software and distribute malware to consumers.[5][6]

3CX also faced backlash for requiring users to pay a fee when opening support tickets during the breach, which led to further public criticism from system administrators and IT professionals.[6]

> "I have been in contact with 3CX and their suggestion is to open a support ticket at £75 per incident. Ludicrous." -wars_t (reddit.com)

References: [edit | edit source]

1. ↑ 1.0 1.1 "ENTERPRISE GRADE PHONE SYSTEM". *3cx.com*. Archived from the original on 2025-08-13. Retrieved 2025-08-13.
2. ↑ Lakshmanan, Ravie (Mar 31, 2023). "3CX Supply Chain Attack — Here's What We Know So Far". *thehackernews.com*. Archived from the original on June 27, 2025. Retrieved 2025-08-12.
3. ↑ "My 3CX Partnership Deleted and All Linked Clients Lost".
4. ↑ "Banned from the 3CX Community".
5. ↑ Greenberg, Andy (Apr 20, 2023). "The Huge 3CX Breach Was Actually 2 Linked Supply Chain Attacks". *Wired*. pp. 2025-08-12. Archived from the original on July 26, 2025.
6. ↑ 6.0 6.1 CrowdStrike (2023-03-29). "// 2023-03-29 // SITUATIONAL AWARENESS // CrowdStrike Tracking Active Intrusion Campaign Targeting 3CX Customers //" . *reddit*.

Categories: Articles in need of additional work | Articles requiring expansion | 3CX

This page was last edited on 25 August 2025, at 04:05.

Privacy policy About Consumer Rights Wiki Disclaimers Mobile view

Powered by MediaWiki