НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220214.16 | 14 февраля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в TP-Link AC1750

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	AC1750: до 211210
Дата выявления	14 февраля 2022 г.
Дата обновления	14 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-24352 CVE-2022-24353	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение	8.8

MITRE: CVE-2022-24354	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение	8.8

Ссылки на источники	http://www.zerodayinitiative.com/advisories/ZDI-22-262/ http://www.zerodayinitiative.com/advisories/ZDI-22-264/ http://www.zerodayinitiative.com/advisories/ZDI-22-263/ https://www.cybersecurity-help.cz/vdb/SB2022021403