RED Check

ОТЧЁТ

№ отчёта	*6debe2fd-ebf7-4ccc-8fd8-dd63c8109655*
Профиль	*Аудит в режиме "Пентест"*
Задание	*KKB2_10.1.6.0*
Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:30:46*
Формирование отчёта	*31.05.2024 12:44:24*
Имя	*KKB2_10.1.6.0*
Хосты [253]	*10.1.6.1, 10.1.6.2, 10.1.6.3, 10.1.6.4, 10.1.6.5, 10.1.6.6, 10.1.6.7, 10.1.6.8, 10.1.6.9, 10.1.6.10, 10.1.6.11, 10.1.6.12, 10.1.6.13, 10.1.6.14, 10.1.6.15, 10.1.6.16, 10.1.6.17, 10.1.6.18, 10.1.6.19, 10.1.6.20, 10.1.6.21, 10.1.6.22, 10.1.6.23, 10.1.6.24, 10.1.6.25, 10.1.6.26, 10.1.6.27, 10.1.6.28, 10.1.6.29, 10.1.6.30, 10.1.6.31, 10.1.6.32, 10.1.6.33, 10.1.6.34, 10.1.6.35, 10.1.6.36, 10.1.6.37, 10.1.6.38, 10.1.6.39, 10.1.6.40, 10.1.6.41, 10.1.6.42, 10.1.6.43, 10.1.6.44, 10.1.6.45, 10.1.6.46, 10.1.6.47, 10.1.6.48, 10.1.6.49, 10.1.6.50, 10.1.6.51, 10.1.6.52, 10.1.6.53, 10.1.6.54, 10.1.6.55, 10.1.6.56, 10.1.6.57, 10.1.6.58, 10.1.6.59, 10.1.6.60, 10.1.6.61, 10.1.6.62, 10.1.6.63, 10.1.6.64, 10.1.6.65, 10.1.6.66, 10.1.6.67, 10.1.6.68, 10.1.6.69, 10.1.6.70, 10.1.6.71, 10.1.6.72, 10.1.6.73, 10.1.6.74, 10.1.6.75, 10.1.6.76, 10.1.6.77, 10.1.6.78, 10.1.6.79, 10.1.6.80, 10.1.6.81, 10.1.6.82, 10.1.6.83, 10.1.6.84, 10.1.6.85, 10.1.6.86, 10.1.6.87, 10.1.6.88, 10.1.6.89, 10.1.6.90, 10.1.6.91, 10.1.6.92, 10.1.6.93, 10.1.6.94, 10.1.6.95, 10.1.6.96, 10.1.6.97, 10.1.6.98, 10.1.6.99, 10.1.6.100, 10.1.6.101, 10.1.6.102, 10.1.6.103, 10.1.6.104, 10.1.6.105, 10.1.6.106, 10.1.6.107, 10.1.6.108, 10.1.6.109, 10.1.6.110, 10.1.6.111, 10.1.6.112, 10.1.6.113, 10.1.6.114, 10.1.6.115, 10.1.6.116, 10.1.6.117, 10.1.6.118, 10.1.6.119, 10.1.6.120, 10.1.6.121, 10.1.6.122, 10.1.6.123, 10.1.6.124, 10.1.6.125, 10.1.6.126, 10.1.6.127, 10.1.6.128, 10.1.6.129, 10.1.6.130, 10.1.6.131, 10.1.6.132, 10.1.6.133, 10.1.6.134, 10.1.6.135, 10.1.6.136, 10.1.6.137, 10.1.6.138, 10.1.6.139, 10.1.6.140, 10.1.6.141, 10.1.6.142, 10.1.6.143, 10.1.6.144, 10.1.6.145, 10.1.6.146, 10.1.6.147, 10.1.6.148, 10.1.6.149, 10.1.6.150, 10.1.6.151, 10.1.6.152, 10.1.6.153, 10.1.6.154, 10.1.6.155, 10.1.6.156, 10.1.6.157, 10.1.6.158, 10.1.6.159, 10.1.6.160, 10.1.6.161, 10.1.6.162, 10.1.6.163, 10.1.6.164, 10.1.6.165, 10.1.6.166, 10.1.6.167, 10.1.6.168, 10.1.6.169, 10.1.6.170, 10.1.6.171, 10.1.6.172, 10.1.6.173, 10.1.6.174, 10.1.6.175, 10.1.6.176, 10.1.6.177, 10.1.6.178, 10.1.6.179, 10.1.6.180, 10.1.6.181, 10.1.6.182, 10.1.6.183, 10.1.6.184, 10.1.6.185, 10.1.6.186, 10.1.6.187, 10.1.6.188, 10.1.6.189, 10.1.6.190, 10.1.6.191, 10.1.6.192, 10.1.6.193, 10.1.6.194, 10.1.6.195, 10.1.6.196, 10.1.6.197, 10.1.6.198, 10.1.6.199, 10.1.6.200, 10.1.6.201, 10.1.6.202, 10.1.6.203, 10.1.6.204, 10.1.6.205, 10.1.6.206, 10.1.6.207, 10.1.6.208, 10.1.6.209, 10.1.6.210, 10.1.6.211, 10.1.6.212, 10.1.6.213, 10.1.6.214, 10.1.6.215, 10.1.6.216, 10.1.6.217, 10.1.6.218, 10.1.6.219, 10.1.6.220, 10.1.6.221, 10.1.6.222, 10.1.6.223, 10.1.6.224, 10.1.6.225, 10.1.6.226, 10.1.6.227, 10.1.6.228, 10.1.6.229, 10.1.6.230, 10.1.6.231, 10.1.6.232, 10.1.6.233, 10.1.6.234, 10.1.6.235, 10.1.6.236, 10.1.6.237, 10.1.6.238, 10.1.6.239, 10.1.6.240, 10.1.6.241, 10.1.6.242, 10.1.6.243, 10.1.6.244, 10.1.6.245, 10.1.6.246, 10.1.6.247, 10.1.6.248, 10.1.6.249, 10.1.6.250, 10.1.6.251, 10.1.6.252, 10.1.6.253*

Хост: 10.1.6.1

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.1

Хост: 10.1.6.2

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.2

Хост: 10.1.6.3

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.3

Хост: 10.1.6.4

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.4

Хост: 10.1.6.5

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.5

Хост: 10.1.6.6

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.6

Хост: 10.1.6.7

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.7

Хост: 10.1.6.8

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.8

Хост: 10.1.6.9

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.9

Хост: 10.1.6.10

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.10

Хост: 10.1.6.11

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:01*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Продукты [1]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
4899	tcp	Информация	radmin	Radmin Authentication

Метод определения	*Probed*
Продукты	*cpe:/a:famatech:radmin:3.X*
Дополнительно	*Radmin Authentication*

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.11
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.12

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:01*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.12	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.12	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:10*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:10*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	skreg-6okno.kmldo.local
	IPv4-адрес	10.1.6.12
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.13

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.13

Хост: 10.1.6.14

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.14

Хост: 10.1.6.15

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:01*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.15	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.15	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:10*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:10*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	regpc-o3.kmldo.local
	IPv4-адрес	10.1.6.15
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.16

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.16

Хост: 10.1.6.17

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.17

Хост: 10.1.6.18

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.18

Хост: 10.1.6.19

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.19

Хост: 10.1.6.20

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.20

Хост: 10.1.6.21

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.21

Хост: 10.1.6.22

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.22

Хост: 10.1.6.23

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.23

Хост: 10.1.6.24

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.24

Хост: 10.1.6.25

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:01*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Продукты [2]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	321-kons-k401-1.kmldo.local
	IPv4-адрес	10.1.6.25
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.26

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.26

Хост: 10.1.6.27

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:01*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.27	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.27	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:11*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:11*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	jk5reg-1.kmldo.local
	IPv4-адрес	10.1.6.27
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.28

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.28

Хост: 10.1.6.29

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	cz-eko-k6-3.kmldo.local
	IPv4-адрес	10.1.6.29

Хост: 10.1.6.30

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.30

Хост: 10.1.6.31

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.31

Хост: 10.1.6.32

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.32

Хост: 10.1.6.33

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.33

Хост: 10.1.6.34

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:02*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [130]

Хост	CVE	Риск	Описание
10.1.6.34	CVE-2022-2068	Критический	Уязвимость в OpenSSL 3.0.0, 3.0.1, 3.0.2, 3.0.3, 1.1.1 до 1.1.1o, и 1.0.2 до 1.0.2ze позволяет злоумышленнику выполнить...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.16*		
10.1.6.34	CVE-2022-2068	Критический	Уязвимость в OpenSSL 3.0.0, 3.0.1, 3.0.2, 3.0.3, 1.1.1 до 1.1.1o, и 1.0.2 до 1.0.2ze позволяет злоумышленнику выполнить...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.16*		
10.1.6.34	CVE-2022-22720	Высокий	Проникновение HTTP-запроса (HRS) в Apache HTTP Server 2.4.52 и ниже.
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.52*		
10.1.6.34	CVE-2021-44790	Высокий	Переполнение буфера в mod_lua в Apache HTTP Server версии с 2.4 до 2.4.51.
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server = 2.4.51*		
10.1.6.34	CVE-2022-23943	Высокий	Уязвимость записи за пределами выделенной памяти в mod_sed в Apache HTTP Server позволяет злоумышленникам перезаписать...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.52*		
10.1.6.34	CVE-2022-31813	Высокий	Apache HTTP Server 2.4.53 и более ранние версии могут не отправлять заголовки X-Forwarded-* на исходный сервер...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	ALTXID-335831	Высокий	Включён режим отладки для приложений ASP.NET. Отключите режим отладки для приложений ASP.NET.

Продукты	*cpe:/a:apache:http_server:2.4.51*
Порт	*80 (tcp)*
Точность	*Высокая*
Детализация	*status: DEBUG is enabled (http-aspnet-debug)*

10.1.6.34	CVE-2017-8923	Высокий	Функция zend_string_extend в Zend/zend_string.h в PHP по 7.1.5 позволяет удалённым злоумышленникам вызвать отказ...

Продукты	*cpe:/a:php:php:7.4.9*
Порт	*80 (tcp)*
Точность	*Высокая*
Детализация	*php:php < 7.4.24*

10.1.6.34	CVE-2017-9120	Высокий	PHP 7.x по 7.1.5 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (переполнение буфера и падение...

Продукты	*cpe:/a:php:php:7.4.9*
Порт	*80 (tcp)*
Точность	*Высокая*
Детализация	*php:php > 7.4.0 & php:php < 7.4.23*

10.1.6.34	CVE-2022-22720	Высокий	Проникновение HTTP-запроса (HRS) в Apache HTTP Server 2.4.52 и ниже.

Продукты	*cpe:/a:apache:http_server:2.4.51*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*apache:http_server < 2.4.52*

10.1.6.34	CVE-2021-44790	Высокий	Переполнение буфера в mod_lua в Apache HTTP Server версии с 2.4 до 2.4.51.

Продукты	*cpe:/a:apache:http_server:2.4.51*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*apache:http_server = 2.4.51*

10.1.6.34	CVE-2022-23943	Высокий	Уязвимость записи за пределами выделенной памяти в mod_sed в Apache HTTP Server позволяет злоумышленникам перезаписать...

Продукты	*cpe:/a:apache:http_server:2.4.51*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.52*

10.1.6.34	CVE-2022-31813	Высокий	Apache HTTP Server 2.4.53 и более ранние версии могут не отправлять заголовки X-Forwarded-* на исходный сервер...

Продукты	*cpe:/a:apache:http_server:2.4.51*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*apache:http_server < 2.4.53*

10.1.6.34	ALTXID-335831	Высокий	Включён режим отладки для приложений ASP.NET. Отключите режим отладки для приложений ASP.NET.

Продукты	*cpe:/a:apache:http_server:2.4.51*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*status: DEBUG is enabled (http-aspnet-debug)*

10.1.6.34	CVE-2017-8923	Высокий	Функция zend_string_extend в Zend/zend_string.h в PHP по 7.1.5 позволяет удалённым злоумышленникам вызвать отказ...

Продукты	*cpe:/a:php:php:7.4.9*
Порт	*443 (tcp)*

Точность	*Высокая*		
Детализация	*php:php < 7.4.24*		
10.1.6.34	CVE-2017-9120	Высокий	PHP 7.x по 7.1.5 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (переполнение буфера и падение...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.23*		
10.1.6.34	CVE-2022-28330	Средний	Apache HTTP Server 2.4.53 и более ранних версий в Windows может читать за пределами выделенной памяти, если он...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-30556	Средний	Apache HTTP Server 2.4.53 и более ранние версии могут возвращать приложениям, вызывающим r:wsread(), длины, которые...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-29404	Средний	В Apache HTTP Server 2.4.53 и более ранних версиях вредоносный запрос к скрипту lua, вызывающему r:parsebody (0),...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2021-44224	Средний	Уязвимость в Apache HTTP Server версии с 2.4.7 до 2.4.51 при включенном ProxyRequests может вызвать падение (разыменование...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.7 & apache:http_server < 2.4.52*		
10.1.6.34	CVE-2022-28615	Средний	Apache HTTP Server 2.4.53 и более ранние версии могут аварийно завершить работу или раскрыть информацию из-за чтения...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-22719	Средний	Уязвимость в Apache HTTP Server до 2.4.52 может привести к сбою процесса из-за специально сформированного тела...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.52*		
10.1.6.34	CVE-2022-26377	Средний	Уязвимость «Несогласованная интерпретация HTTP-запросов» («Контрабанда HTTP-запросов») в mod_proxy_ajp сервера...
Продукты	*cpe:/a:apache:http_server:2.4.51*		

Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-28614	Средний	Функция ap_rwrite() в Apache HTTP Server 2.4.53 и более ранних версиях может считывать память, если злоумышленник...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-22721	Средний	Целочисленное переполнение в Apache HTTP Server до 2.4.52.
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.52*		
10.1.6.34	ALTXID-340429	Средний	Обнаружены резервные копии файлов на веб сервере. Не рекомендуется хранить бэкапы на том же диске, что и исходные...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*withinhost=10.1.6.34 http://10.1.6.34:80/js/app.bak http://10.1.6.34:80/js/app.js~ http://10.1.6.34:80/js/app copy.js http://10.1.6.34:80/js/Copy of app.js http://10.1.6.34:80/js/Copy (2) of app.js http://10.1.6.34:80/js/app.js.1 http://10.1.6.34:80/js/app.js.~1~ (http-backup-finder)*		
10.1.6.34	ALTXID-338287	Средний	Обнаружен потенциально опасный http метод TRACE. Этот метод возвращает в ответе клиенту строку, которая была ему...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*TRACE is enabledHeaders:Date: Fri, 31 May 2024 09:04:43 GMTServer: Apache/2.4.51 (Win64) OpenSSL/1.1.1g PHP/7.4.9Connection: closeTransfer-Encoding: chunkedContent-Type: message/http (http-trace)*		
10.1.6.34	CVE-2017-9118	Средний	Доступ за пределами выделенной памяти в php_pcre_replace_impl в PHP 7.1.5 через специально сформированный preg_replace...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.27*		
10.1.6.34	CVE-2020-7071	Средний	В версиях PHP 7.3.x ниже 7.3.26, 7.4.x ниже 7.4.14 и 8.0.0 при проверке URL-адреса с помощью таких функций, как...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.14*		
10.1.6.34	CVE-2021-21702	Средний	В версиях PHP 7.3.x ниже 7.3.27, 7.4.x ниже 7.4.15 и 8.0.x ниже 8.0.2 при использовании расширения SOAP для подключения...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.15*		
10.1.6.34	CVE-2021-21706	Средний	Уязвимость в PHP версии 7.3.x до 7.3.31, 7.4.x до 7.4.24 и 8.0.x до 8.0.11, в ZipArchive::extractTo может привести...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		

Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.24*		
10.1.6.34	CVE-2021-21705	Средний	Уязвимость в PHP версии 7.3.x до 7.3.29, 7.4.x до 7.4.21 и 8.0.x до 8.0.8 при проверке URL.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.21*		
10.1.6.34	CVE-2021-21704	Средний	Уязвимость в PHP версии 7.3.x до 7.3.29, 7.4.x до 7.4.21 и 8.0.x до 8.0.8 при использовании Firebird PDO драйвера...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.21*		
10.1.6.34	CVE-2021-21708	Средний	В версиях PHP 7.4.x ниже 7.4.28, 8.0.x ниже 8.0.16 и 8.1.x ниже 8.1.3 при использовании функций фильтра с фильтром...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.28*		
10.1.6.34	CVE-2021-21707	Средний	В PHP версии 7.3.x до 7.3.33, 7.4.x до 7.4.26 и 8.0.x до 8.0.13 некоторые функции анализа XML, такие как simplexml_load_file (),...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.26*		
10.1.6.34	CVE-2022-31625	Средний	Использование неинициализированной памяти в pg_query_params() в PHP до 8.0.20 и до 8.1.7 и до 7.4.30.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.30*		
10.1.6.34	CVE-2021-21703	Средний	Уязвимость повреждения памяти в PHP до 8.0.12 и до 7.3.32 и до 7.4.25 позволяет повысить привилегии.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.25*		
10.1.6.34	CVE-2020-7070	Средний	Уязвимость в обработке значений HTTP cookie в PHP версии 7.2.x до 7.2.34, 7.3.x до 7.3.23 и 7.4.x до 7.4.11 позволяет...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.11*		
10.1.6.34	CVE-2022-31626	Средний	Переполнение буфера в PHP до 8.0.20 и до 8.1.7 и до 7.4.30.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.30*		
10.1.6.34	CVE-2020-7069	Средний	Уязвимость в PHP версии 7.2.x до 7.2.34, 7.3.x до 7.3.23 и 7.4.x до 7.4.11, когда AES-CCM mode используется, может...

Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.11*		
10.1.6.34	CVE-2021-23840	Средний	Уязвимость в EVP_CipherUpdate, EVP_EncryptUpdate и EVP_DecryptUpdate в OpenSSL 1.1.1 до 1.1.1i, и 1.0.2 до 1.0.2x...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.10*		
10.1.6.34	CVE-2021-3712	Средний	Уязвимость в OpenSSL 1.1.1 до 1.1.1k, и 1.0.2 до 1.0.2y может вызвать атаку "Отказ в обслуживании", а также привести...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.12*		
10.1.6.34	CVE-2021-4160	Средний	OpenSSL 1.0.2, 1.1.1 и 3.0.0. В процедуре возведения в квадрат MIPS32 и MIPS64 обнаружена ошибка распространения...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.13*		
10.1.6.34	CVE-2019-0190	Средний	Уязвимость в Apache HTTP Server версии 2.4.37.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1*		
10.1.6.34	CVE-2020-15400	Средний	CakePHP до 4.0.6 неправильно обрабатывает генерацию токенов CSRF. Это может быть удаленно использовано вместе с...
Продукты	*cpe:/a:cakefoundation:cakephp:1.1*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*cakefoundation:cakephp < 4.0.6*		
10.1.6.34	CVE-2006-5031	Средний	Уязвимость обхода каталогов в app/webroot/js/vendors.php в Cake Software Foundation CakePHP до 1.1.8.3544 позволяет...
Продукты	*cpe:/a:cakefoundation:cakephp:1.1*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*cakefoundation:cakephp < 1.1.7.3363*		
10.1.6.34	CVE-2006-4067	Средний	Уязвимость межсайтового скриптинга в cake/libs/error.php в CakePHP до 1.1.7.3363 позволяет внедрять произвольный...
Продукты	*cpe:/a:cakefoundation:cakephp:1.1*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*cakefoundation:cakephp < 1.1.6.3264*		
10.1.6.34	CVE-2022-28330	Средний	Apache HTTP Server 2.4.53 и более ранних версий в Windows может читать за пределами выделенной памяти, если он...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		

Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-30556	Средний	Apache HTTP Server 2.4.53 и более ранние версии могут возвращать приложениям, вызывающим r:wsread(), длины, которые...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-29404	Средний	В Apache HTTP Server 2.4.53 и более ранних версиях вредоносный запрос к скрипту lua, вызывающему r:parsebody (0),...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2021-44224	Средний	Уязвимость в Apache HTTP Server версии с 2.4.7 до 2.4.51 при включенном ProxyRequests может вызвать падение (разыменование...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.7 & apache:http_server < 2.4.52*		
10.1.6.34	CVE-2022-28615	Средний	Apache HTTP Server 2.4.53 и более ранние версии могут аварийно завершить работу или раскрыть информацию из-за чтения...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-22719	Средний	Уязвимость в Apache HTTP Server до 2.4.52 может привести к сбою процесса из-за специально сформированного тела...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.52*		
10.1.6.34	CVE-2022-26377	Средний	Уязвимость «Несогласованная интерпретация HTTP-запросов» («Контрабанда HTTP-запросов») в mod_proxy_ajp сервера...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-28614	Средний	Функция ap_rwrite() в Apache HTTP Server 2.4.53 и более ранних версиях может считывать память, если злоумышленник...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.53*		
10.1.6.34	CVE-2022-22721	Средний	Целочисленное переполнение в Apache HTTP Server до 2.4.52.
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		

Детализация	*apache:http_server < 2.4.52*		
10.1.6.34	ALTXID-338287	Средний	Обнаружен потенциально опасный http метод TRACE. Этот метод возвращает в ответе клиенту строку, которая была ему...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*TRACE is enabledHeaders:Date: Fri, 31 May 2024 09:04:43 GMTServer: Apache/2.4.51 (Win64) OpenSSL/1.1.1g PHP/7.4.9Connection: closeTransfer-Encoding: chunkedContent-Type: message/http (http-trace)*		
10.1.6.34	CVE-2017-9118	Средний	Доступ за пределами выделенной памяти в php_pcre_replace_impl в PHP 7.1.5 через специально сформированный preg_replace...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.27*		
10.1.6.34	CVE-2020-7071	Средний	В версиях PHP 7.3.x ниже 7.3.26, 7.4.x ниже 7.4.14 и 8.0.0 при проверке URL-адреса с помощью таких функций, как...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.14*		
10.1.6.34	CVE-2021-21702	Средний	В версиях PHP 7.3.x ниже 7.3.27, 7.4.x ниже 7.4.15 и 8.0.x ниже 8.0.2 при использовании расширения SOAP для подключения...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.15*		
10.1.6.34	CVE-2021-21706	Средний	Уязвимость в PHP версии 7.3.x до 7.3.31, 7.4.x до 7.4.24 и 8.0.x до 8.0.11, в ZipArchive::extractTo может привести...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.24*		
10.1.6.34	CVE-2021-21705	Средний	Уязвимость в PHP версии 7.3.x до 7.3.29, 7.4.x до 7.4.21 и 8.0.x до 8.0.8 при проверке URL.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.21*		
10.1.6.34	CVE-2021-21704	Средний	Уязвимость в PHP версии 7.3.x до 7.3.29, 7.4.x до 7.4.21 и 8.0.x до 8.0.8 при использовании Firebird PDO драйвера...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.21*		
10.1.6.34	CVE-2021-21708	Средний	В версиях PHP 7.4.x ниже 7.4.28, 8.0.x ниже 8.0.16 и 8.1.x ниже 8.1.3 при использовании функций фильтра с фильтром...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.28*		

10.1.6.34	CVE-2021-21707	Средний	В PHP версии 7.3.x до 7.3.33, 7.4.x до 7.4.26 и 8.0.x до 8.0.13 некоторые функции анализа XML, такие как simplexml_load_file (),...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.26*		
10.1.6.34	CVE-2022-31625	Средний	Использование неинициализированной памяти в pg_query_params() в PHP до 8.0.20 и до 8.1.7 и до 7.4.30.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.30*		
10.1.6.34	CVE-2021-21703	Средний	Уязвимость повреждения памяти в PHP до 8.0.12 и до 7.3.32 и до 7.4.25 позволяет повысить привилегии.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.25*		
10.1.6.34	CVE-2020-7070	Средний	Уязвимость в обработке значений HTTP cookie в PHP версии 7.2.x до 7.2.34, 7.3.x до 7.3.23 и 7.4.x до 7.4.11 позволяет...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.11*		
10.1.6.34	CVE-2022-31626	Средний	Переполнение буфера в PHP до 8.0.20 и до 8.1.7 и до 7.4.30.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.30*		
10.1.6.34	CVE-2020-7069	Средний	Уязвимость в PHP версии 7.2.x до 7.2.34, 7.3.x до 7.3.23 и 7.4.x до 7.4.11, когда AES-CCM mode используется, может...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.11*		
10.1.6.34	CVE-2021-23840	Средний	Уязвимость в EVP_CipherUpdate, EVP_EncryptUpdate и EVP_DecryptUpdate в OpenSSL 1.1.1 до 1.1.1i, и 1.0.2 до 1.0.2x...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.10*		
10.1.6.34	CVE-2021-3712	Средний	Уязвимость в OpenSSL 1.1.1 до 1.1.1k, и 1.0.2 до 1.0.2y может вызвать атаку "Отказ в обслуживании", а также привести...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.12*		
10.1.6.34	CVE-2021-4160	Средний	OpenSSL 1.0.2, 1.1.1 и 3.0.0. В процедуре возведения в квадрат MIPS32 и MIPS64 обнаружена ошибка распространения...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		

Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.13*		
10.1.6.34	CVE-2019-0190	Средний	Уязвимость в Apache HTTP Server версии 2.4.37.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1*		
10.1.6.34	CVE-2019-1551	Средний	Ошибка переполнения в OpenSSL 1.1.1-1.1.1d и 1.0.2-1.0.2t.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2018-0735	Средний	Уязвимость в алгоритме подписи OpenSSL ECDSA, злоумышленник может использовать различные варианты алгоритма подписи...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1563	Средний	Уязвимость в OpenSSL до 1.1.1d, до 1.1.0l и до 1.0.2t позволяет восстановить CMS/PKCS7 транспортированный ключ...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1549	Средний	OpenSSL до 1.1.1d не использовал по умолчанию генератор случайных чисел (RNG) для защиты в случае системного вызова...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1543	Средний	Раскрытие информации в OpenSSL в шифре ChaCha20-Poly1305. Уязвимы версии 1.1.1 до 1.1.1b, и 1.1.0 до 1.1.0j.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1551	Средний	Ошибка переполнения в OpenSSL 1.1.1-1.1.1d и 1.0.2-1.0.2t.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2018-0735	Средний	Уязвимость в алгоритме подписи OpenSSL ECDSA, злоумышленник может использовать различные варианты алгоритма подписи...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		

10.1.6.34	CVE-2019-1563	Средний	Уязвимость в OpenSSL до 1.1.1d, до 1.1.0l и до 1.0.2t позволяет восстановить CMS/PKCS7 транспортированный ключ...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1549	Средний	OpenSSL до 1.1.1d не использовал по умолчанию генератор случайных чисел (RNG) для защиты в случае системного вызова...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1543	Средний	Раскрытие информации в OpenSSL в шифре ChaCha20-Poly1305. Уязвимы версии 1.1.1 до 1.1.1b, и 1.1.0 до 1.1.0j.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1552	Низкий	OpenSSL имеет внутреннее значение по умолчанию для дерева каталогов, где он может найти файлы конфигурации и сертификаты....
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2019-1552	Низкий	OpenSSL имеет внутреннее значение по умолчанию для дерева каталогов, где он может найти файлы конфигурации и сертификаты....
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2006-20001	Недоступно	Тщательно созданный заголовок запроса If: может привести к считыванию или записи одного нулевого байта в ячейку...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.55*		
10.1.6.34	CVE-2023-25690	Недоступно	Некоторые конфигурации mod_proxy, если он включен вместе с какой-либо формой RewriteRule или ProxyPassMatch, на...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.55*		
10.1.6.34	CVE-2023-27522	Недоступно	Уязвимость для контрабанды HTTP-ответов в HTTP-сервере Apache через mod_proxy_uwsgi (HTTP-сервер Apache с 2.4.30...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.30 & apache:http_server < 2.4.55*		

10.1.6.34	CVE-2022-36760	Недоступно	Уязвимость "контрабанды HTTP-запросов" в mod_proxy_ajp HTTP-сервера Apache позволяет переправлять запросы на сервер...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.55*		
10.1.6.34	CVE-2022-37436	Недоступно	Apache HTTP Server до 2.4.55, вредоносная серверная часть могла привести к преждевременному усечению заголовков...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.55*		
10.1.6.34	CVE-2023-45802	Недоступно	Когда поток HTTP/2 был сброшен клиентом (RST кадр), возникло временное окно, в течение которого ресурсы памяти...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.58*		
10.1.6.34	CVE-2023-31122	Недоступно	Уязвимость для чтения за пределами доступа в mod_macro HTTP-сервера Apache.Эта проблема затрагивает HTTP-сервер...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.57*		
10.1.6.34	CVE-2022-37454	Недоступно	Переполнение буфера в Keccak XKCP SHA-3 реализации до 8.0.25 и до 8.1.12 позволяет удалённым злоумышленникам выполнить...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.33*		
10.1.6.34	CVE-2022-31628	Недоступно	Бесконечный цикл в PHP до 7.4.31, 8.0.24 и 8.1.11 при распаковке gzip "quines" файлов.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.32*		
10.1.6.34	CVE-2022-31630	Недоступно	Уязвимость проверки входных данных в imageloadfont() до 8.0.25 и до 8.1.12.
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.33*		
10.1.6.34	CVE-2022-31629	Недоступно	Уязвимость в PHP до 8.0.24 и до 8.1.11 и до 7.4.32 позволяет сайтам злоумышленников установить небезопасный cookie...
Продукты	*cpe:/a:php:php:7.4.9*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*php:php > 7.4.0 & php:php < 7.4.32*		
10.1.6.34	CVE-2023-3817	Недоступно	Отказ в обслуживании в pip пакете cryptography до 41.0.3.

Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl = 1.1.1g*		
10.1.6.34	CVE-2023-0466	Недоступно	Функция X509_VERIFY_PARAM_add0_policy() документирована для неявного включения проверки политики сертификата при...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.21*		
10.1.6.34	CVE-2022-4450	Недоступно	Уязвимость двойного освобождения в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t может привести к падению приложения.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.20*		
10.1.6.34	CVE-2024-0727	Недоступно	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.24*		
10.1.6.34	CVE-2022-4304	Недоступно	Уязвимость в IBM Semeru до 8.0.362 и до 11.0.18 и до 17.0.6.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.20*		
10.1.6.34	CVE-2023-0286	Недоступно	Уязвимость, связанная с подменой типа в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t при обработке X.509 GeneralName...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.20*		
10.1.6.34	CVE-2023-0465	Недоступно	Приложения, использующие при проверке сертификатов опции не по умолчанию, могут быть уязвимы для атаки со стороны...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.21*		
10.1.6.34	CVE-2023-5678	Недоступно	Генерация чрезмерно длинных ключей X9.42 DH или проверка чрезмерно длинных ключей или параметров X9.42 DH может...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.24*		
10.1.6.34	CVE-2023-0464	Недоступно	Уязвимость в OpenSSL 3.1.0 до 3.1.1, 3.0.0 до 3.0.9, и 1.1.1 до 1.1.1u, связанная с проверкой X.509 сертификата,...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.21*		

10.1.6.34	CVE-2023-4807	Недоступно	Отказ в обслуживании в pip пакете cryptography до 41.0.4.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.23*		
10.1.6.34	CVE-2006-20001	Недоступно	Тщательно созданный заголовок запроса If: может привести к считыванию или записи одного нулевого байта в ячейку...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.55*		
10.1.6.34	CVE-2023-25690	Недоступно	Некоторые конфигурации mod_proxy, если он включен вместе с какой-либо формой RewriteRule или ProxyPassMatch, на...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.55*		
10.1.6.34	CVE-2023-27522	Недоступно	Уязвимость для контрабанды HTTP-ответов в HTTP-сервере Apache через mod_proxy_uwsgi (HTTP-сервер Apache с 2.4.30...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.30 & apache:http_server < 2.4.55*		
10.1.6.34	CVE-2022-36760	Недоступно	Уязвимость "контрабанды HTTP-запросов" в mod_proxy_ajp HTTP-сервера Apache позволяет переправлять запросы на сервер...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server > 2.4.0 & apache:http_server < 2.4.55*		
10.1.6.34	CVE-2022-37436	Недоступно	Apache HTTP Server до 2.4.55, вредоносная серверная часть могла привести к преждевременному усечению заголовков...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.55*		
10.1.6.34	CVE-2023-45802	Недоступно	Когда поток HTTP/2 был сброшен клиентом (RST кадр), возникло временное окно, в течение которого ресурсы памяти...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.58*		
10.1.6.34	CVE-2023-31122	Недоступно	Уязвимость для чтения за пределами доступа в mod_macro HTTP-сервера Apache.Эта проблема затрагивает HTTP-сервер...
Продукты	*cpe:/a:apache:http_server:2.4.51*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*apache:http_server < 2.4.57*		
10.1.6.34	CVE-2022-37454	Недоступно	Переполнение буфера в Keccak XKCP SHA-3 реализации до 8.0.25 и до 8.1.12 позволяет удалённым злоумышленникам выполнить...

Продукты	*cpe:/a:php:php:7.4.9*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*php:php > 7.4.0 & php:php < 7.4.33*

10.1.6.34	CVE-2022-31628	Недоступно	Бесконечный цикл в PHP до 7.4.31, 8.0.24 и 8.1.11 при распаковке gzip "quines" файлов.

Продукты	*cpe:/a:php:php:7.4.9*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*php:php > 7.4.0 & php:php < 7.4.32*

10.1.6.34	CVE-2022-31630	Недоступно	Уязвимость проверки входных данных в imageloadfont() до 8.0.25 и до 8.1.12.

Продукты	*cpe:/a:php:php:7.4.9*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*php:php > 7.4.0 & php:php < 7.4.33*

10.1.6.34	CVE-2022-31629	Недоступно	Уязвимость в PHP до 8.0.24 и до 8.1.11 и до 7.4.32 позволяет сайтам злоумышленников установить небезопасный cookie...

Продукты	*cpe:/a:php:php:7.4.9*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*php:php > 7.4.0 & php:php < 7.4.32*

10.1.6.34	CVE-2023-3817	Недоступно	Отказ в обслуживании в pip пакете cryptography до 41.0.3.

Продукты	*cpe:/a:openssl:openssl:1.1.1g*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*openssl:openssl = 1.1.1g*

10.1.6.34	CVE-2023-0466	Недоступно	Функция X509_VERIFY_PARAM_add0_policy() документирована для неявного включения проверки политики сертификата при...

Продукты	*cpe:/a:openssl:openssl:1.1.1g*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.21*

10.1.6.34	CVE-2022-4450	Недоступно	Уязвимость двойного освобождения в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t может привести к падению приложения.

Продукты	*cpe:/a:openssl:openssl:1.1.1g*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.20*

10.1.6.34	CVE-2024-0727	Недоступно	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential...

Продукты	*cpe:/a:openssl:openssl:1.1.1g*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.24*

10.1.6.34	CVE-2022-4304	Недоступно	Уязвимость в IBM Semeru до 8.0.362 и до 11.0.18 и до 17.0.6.

Продукты	*cpe:/a:openssl:openssl:1.1.1g*
Порт	*443 (tcp)*
Точность	*Высокая*
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.20*

10.1.6.34	CVE-2023-0286	Недоступно	Уязвимость, связанная с подменой типа в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t при обработке X.509 GeneralName...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.20*		
10.1.6.34	CVE-2023-0465	Недоступно	Приложения, использующие при проверке сертификатов опции не по умолчанию, могут быть уязвимы для атаки со стороны...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.21*		
10.1.6.34	CVE-2023-5678	Недоступно	Генерация чрезмерно длинных ключей X9.42 DH или проверка чрезмерно длинных ключей или параметров X9.42 DH может...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.24*		
10.1.6.34	CVE-2023-0464	Недоступно	Уязвимость в OpenSSL 3.1.0 до 3.1.1, 3.0.0 до 3.0.9, и 1.1.1 до 1.1.1u, связанная с проверкой X.509 сертификата,...
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.21*		
10.1.6.34	CVE-2023-4807	Недоступно	Отказ в обслуживании в pip пакете cryptography до 41.0.4.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Высокая*		
Детализация	*openssl:openssl > 1.1.1 & openssl:openssl < 1.1.1.23*		
10.1.6.34	CVE-2023-3446	Недоступно	Отказ в обслуживании в pip пакете cryptography до 41.0.3.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*80 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		
10.1.6.34	CVE-2023-3446	Недоступно	Отказ в обслуживании в pip пакете cryptography до 41.0.3.
Продукты	*cpe:/a:openssl:openssl:1.1.1g*		
Порт	*443 (tcp)*		
Точность	*Средняя*		
Детализация	*openssl:openssl = 1.1.1*		

Инвентаризация

Продукты [8]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
80	tcp	Высокий	http	(Win64) OpenSSL/1.1.1g PHP/7.4.9
Метод определения	*Probed*			
Продукты	*cpe:/a:apache:http_server:2.4.51*			
Дополнительно	*(Win64) OpenSSL/1.1.1g PHP/7.4.9*			
Поддерживаемые http методы	*Метод*	*GET | HEAD | OPTIONS | TRACE*		

Http заголовки, влияющие на безопасность	*Cache-Control*	*no-cache, private*			
Системное время хоста через http	*Fri, 31 May 2024 09:04:47 GMT; -4m26s from local time.*				
Http заголовки	*Date: Fri, 31 May 2024 09:04:46 GMT* *Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1g PHP/7.4.9* *X-Powered-By: PHP/7.4.9* *Cache-Control: no-cache, private* *Access-Control-Allow-Origin: ** *Access-Control-Expose-Headers: ** *Set-Cookie: XSRF-TOKEN=eyJpdiI6InRSVTNld0JwT2JYN1dHNHNjZU85UHc9PSIsInZhbHVlIjoiSHBtRmtVakdLK01JV1BNMnE3NUFkaFNZSFpOVVBDK1BreEY2MHc2UUgwOUpTQ2hrR2JzbjllUWNvT21oT1E2YmF2NHN1V1ZnUHBlV1doZDludUVldjZzN2pzb0ZrcytFK3h2cWhqMVRmT1Q5MWVIQnVhU2psVFlHdEFNV0h4eWciLCJtYWMiOiI2NGQ5MzlkZmIxMmRmYzEzYWY3NGM4YTk3MTY0ZDA4OGI3NzhhZWYxZjkxZTE0OGI2YmYzMDlhNTRkZWFkNGZmIn0%3D; expires=Fri, 31-May-2024 11:04:47 GMT; Max-Age=7200; path=/; samesite=lax* *Set-Cookie: dreambox_session=eyJpdiI6InZud3k5VWlvYmRoY2Y3bGJOOXU3Rmc9PSIsInZhbHVlIjoiMVVGcVhZZUtuRmxnZ1VvNnBucUNpaHpjNGxhTytsYnNKQSswVHdoOVdCWjVaNEZFd1JwUlBEWXFzWXY0K2tIdTM5VkFHSzlxek95TG1tTGl1RGxzQ21PcC9LRjQrbDBRT295R2N4Qy95V3Y4NmF0L015QlhmQ3U1aEpEMEZGQWliLCJtYWMiOiIyNjUyMzkyODU3OTQ3YmNmZGQyZjcwYjcwZmE3ODM4OWE4NjdhYzZlMzE2ZTAwYTc3NDYzMTA4NTVhNTc0NWM5In0%3D; expires=Fri, 31-May-2024 11:04:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax* *Connection: close* *Content-Type: text/html; charset=UTF-8* *(Request type: HEAD)*			
80	tcp	Высокий	http		
Метод определения	*Probed*				
Продукты	*cpe:/a:php:php:7.4.9*				
80	tcp	Критический	http		
Метод определения	*Probed*				
Продукты	*cpe:/a:openssl:openssl:1.1.1g*				
80	tcp	Средний	http		
Метод определения	*Probed*				
Продукты	*cpe:/a:cakefoundation:cakephp:1.1*				
443	tcp	Высокий	http	(Win64) OpenSSL/1.1.1g PHP/7.4.9	
Метод определения	*Probed*				
Продукты	*cpe:/a:apache:http_server:2.4.51*				
Дополнительно	*(Win64) OpenSSL/1.1.1g PHP/7.4.9*				
Поддерживаемые http методы	*Метод*	*GET | HEAD | OPTIONS | TRACE*			
Http заголовки, влияющие на безопасность	*HTTP Strict Transport Security*	*HSTS not configured in HTTPS Server*			
	Cache-Control	*no-cache, private*			
Системное время хоста через http	*Fri, 31 May 2024 09:04:45 GMT; -4m27s from local time.*				

Http заголовки	*Date: Fri, 31 May 2024 09:04:50 GMT* *Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1g PHP/7.4.9* *X-Powered-By: PHP/7.4.9* *Cache-Control: no-cache, private* *Access-Control-Allow-Origin: ** *Access-Control-Expose-Headers: ** *Set-Cookie: XSRF-TOKEN=eyJpdiI6IlpobWNKTmJLd3pOUkdhU01vclNTeHc9PSIsInZhbHVlIjoiT2g0d1BUS1VOWTFSdjhETE5vdXpuT21GSW14czhQb004UWRGRk54YktRb25GRTNmMldxcUVoY2tRTkNFOEdVOVFNU2IvYjdtakpZdG41MWlwb2hCMVFqckRTcVcyWWN1VUNERE42ekR2aVMyblNQSloxQ0xGK3FManowdEhVSlAiLCJtYWMiOiIzZGE3ZGI5NmVmZjZhMjVlMWNmNjNlMDQ4NTJmMzYxMGQyNzg4MWFkN2I4ODNiMWZkNzc4YmNmNjE4MTgyOTE3In0%3D; expires=Fri, 31-May-2024 11:04:50 GMT; Max-Age=7200; path=/; samesite=lax* *Set-Cookie: dreambox_session=eyJpdiI6Ino2OFd5NllsL2VnNnVMRjI0a3JPRlE9PSIsInZhbHVlIjoiRFU4UExtVS9HVzladjNlM3dxeHM2UDJKSEtqdk1TSWV3U1AvNFpMVVROb DU3S25pS1QwTDRHSDQ5M0NqZGRTMmNVYTVId0JWaVc0a0YzMWFERTlVVWI0dDdRT1RtL0RjeDhZdCtXTVpPS3NVMmdlbHF2QUVJazZ4NGlYWmdUcTAiLCJtYWMiOiI5NzVmMTQ5MzUzNzFjNjZmMmRkZDBkYjQ2YTIwZmYxMGEzYWZmYTU1YjU3Mjg1M2ZlYWQ1MDQ4NjAyOThiN2RhIn0%3D; expires=Fri, 31-May-2024 11:04:50 GMT; Max-Age=7200; path=/; httponly; samesite=lax* *Connection: close* *Content-Type: text/html; charset=UTF-8* *(Request type: HEAD)*

443	tcp	Высокий	http	
Метод определения	*Probed*			
Продукты	*cpe:/a:php:php:7.4.9*			
443	tcp	Критический	http	
Метод определения	*Probed*			
Продукты	*cpe:/a:openssl:openssl:1.1.1g*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.34
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.35

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.35

Хост: 10.1.6.36

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.36

Хост: 10.1.6.37

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.37

Хост: 10.1.6.38

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.38

Хост: 10.1.6.39

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.39

Хост: 10.1.6.40

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.40

Хост: 10.1.6.41

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:02*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [12]

Хост	CVE	Риск	Описание
10.1.6.41	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.41	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.41	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.41\IPC$ (READ)*		
10.1.6.41	CVE-2017-0143	Высокий	SMBv1 сервер в Microsoft Windows Vista SP2; Windows Server 2008 SP2 и R2 SP1; Windows 7 SP1; Windows 8.1; Windows...
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) (smb-vuln-ms17-010)*		
10.1.6.41	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.41	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.41	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.41\IPC$ (READ)*		

10.1.6.41	CVE-2017-0143	Высокий	SMBv1 сервер в Microsoft Windows Vista SP2; Windows Server 2008 SP2 и R2 SP1; Windows 7 SP1; Windows 8.1; Windows...
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) (smb-vuln-ms17-010)*		
10.1.6.41	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.41	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.41	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*start date: 2024-05-31T04:46:33 (smb2-time)*		
10.1.6.41	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*start date: 2024-05-31T04:46:33 (smb2-time)*		

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*2.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T08:58:48*		
	Дата запуска	*2024-05-31T04:46:33*		
Файлы SMB	*\\10.1.6.41\Users\.*	*2009-07-14T03:20:08 | <DIR>*		
	\\10.1.6.41 \Users\..	*2009-07-14T03:20:08 | <DIR>*		
	\\10.1.6.41 \Users\Public	*2009-07-14T03:20:08 | <DIR>*		

	\\10.1.6.41\Users\Public\Documents	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\Downloads	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\Music	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\ntuser.dat	*2020-09-16T08:01:46 | 262144*
	\\10.1.6.41\Users\Public\Pictures	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\Recorded TV	*2010-11-21T12:39:28 | <DIR>*
	\\10.1.6.41\Users\Public\Videos	*2009-07-14T03:20:08 | <DIR>*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

445	tcp	Высокий	microsoft-ds	workgroup: WORKGROUP

Метод определения	*Probed*	
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*	
Дополнительно	*workgroup: WORKGROUP*	
Параметры SMB2	*2.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T08:58:48*
	Дата запуска	*2024-05-31T04:46:33*
Файлы SMB	*\\10.1.6.41\Users\.*	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\..	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\Documents	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\Downloads	*2009-07-14T03:20:08 | <DIR>*

	\\10.1.6.41\Users\Public\Music	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\ntuser.dat	*2020-09-16T08:01:46 | 262144*
	\\10.1.6.41\Users\Public\Pictures	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.41\Users\Public\Recorded TV	*2010-11-21T12:39:28 | <DIR>*
	\\10.1.6.41\Users\Public\Videos	*2009-07-14T03:20:08 | <DIR>*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

49157	tcp	Информация	msrpc
Метод определения	*Probed*		
Продукты	*cpe:/a:microsoft:windows_rpc:*		

Информация о хосте

Общая информация	DNS-имя	OKER-K132-2
	Домен	oker-k132-2
	FQDN	oker-k132-2
	IPv4-адрес	10.1.6.41
	lanmanager	Windows 7 Professional 6.1
	Рабочая группа	WORKGROUP\x00
	Сервер	OKER-K132-2\x00
	Системное время	2024-05-31T11:58:48+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.41\ADMIN$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xB9 Admin

	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.41\C$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1\x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1\xD1\x89\xD0\xB8\xD0\xB9 \xD1\x80\xD0\xB5\xD1\x81\xD1\x83\xD1\x80\xD1\x81
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.41\D$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1\x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1\xD1\x89\xD0\xB8\xD0\xB9 \xD1\x80\xD0\xB5\xD1\x81\xD1\x83\xD1\x80\xD1\x81
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.41\IPC$
	Тип	STYPE_IPC_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xB9 IPC
	Анонимный доступ	READ
	Доступ для текущего пользователя	READ/WRITE
Общая папка	Имя	\\10.1.6.41\Kyocera FS-1040
	Тип	STYPE_PRINTQ
	Комментарий	Kyocera FS-1040 GX
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ
Общая папка	Имя	\\10.1.6.41\print$
	Тип	STYPE_DISKTREE
	Комментарий	\xD0\x94\xD1\x80\xD0\xB0\xD0\xB9\xD0\xB2\xD0\xB5\xD1\x80\xD1\x8B \xD0\xBF\xD1\x80\xD0\xB8\xD0\xBD\xD1\x82\xD0\xB5\xD1\x80\xD0\xBE\xD0\xB2
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ
Общая папка	Имя	\\10.1.6.41\Users
	Тип	STYPE_DISKTREE
	Комментарий	
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ

Хост: 10.1.6.42

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	stolovaya-arm1.kmldo.local
	IPv4-адрес	10.1.6.42

Хост: 10.1.6.43

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.43

Хост: 10.1.6.44

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.44

Хост: 10.1.6.45

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:03*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [10]

Хост	CVE	Риск	Описание
10.1.6.45	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.45	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.45	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.45\IPC$ (READ)*		
10.1.6.45	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.45	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.45	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.45\IPC$ (READ)*		
10.1.6.45	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.45	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

10.1.6.45	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...

Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*
Порт	*139 (tcp)*
Точность	*Высокая*
Детализация	*start date: 2024-05-31T06:30:10 (smb2-time)*

10.1.6.45	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...

Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*start date: 2024-05-31T06:30:10 (smb2-time)*

Инвентаризация

Продукты [7]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	

Метод определения	*Probed*	
Продукты	*cpe:/a:microsoft:windows_rpc:*	

139	tcp	Высокий	netbios-ssn	

Метод определения	*Probed*	
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*	
Параметры SMB2	*2.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:14*
	Дата запуска	*2024-05-31T06:30:10*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

445	tcp	Высокий	microsoft-ds	workgroup: KMLDO

Метод определения	*Probed*
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*

Дополнительно	*workgroup: KMLDO*	
Параметры SMB2	*2.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:14*
	Дата запуска	*2024-05-31T06:30:10*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			
49152	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
49153	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
49154	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			

Информация о хосте

Общая информация	DNS-имя	CZ-OK-K3-2 | cz-ok-k3-2.kmldo.local
	Домен	kmldo.local
	FQDN	CZ-OK-k3-2.kmldo.local
	IPv4-адрес	10.1.6.45
	lanmanager	Windows 7 Professional 6.1
	Рабочая группа	KMLDO\x00
	Сервер	CZ-OK-K3-2\x00
	Системное время	2024-05-31T12:09:13+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.45\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.45\C$
	Анонимный доступ	<none>

Общая папка	Имя	\\10.1.6.45\IPC$
	Анонимный доступ	READ
Общая папка	Имя	\\10.1.6.45\PRINT$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.45\USERS
	Анонимный доступ	<none>

Хост: 10.1.6.46

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:03*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.46	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.46	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:18*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:18*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	217ktmrt-k227-1.kmldo.local
	IPv4-адрес	10.1.6.46
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.47

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.47

Хост: 10.1.6.48

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:03*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.48	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.48	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:16*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:16*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm5.kmldo.local
	IPv4-адрес	10.1.6.48
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.49

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm6.kmldo.local
	IPv4-адрес	10.1.6.49

Хост: 10.1.6.50

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	ok-maimeskulova.kmldo.local
	IPv4-адрес	10.1.6.50

Хост: 10.1.6.51

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.51

Хост: 10.1.6.52

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:03*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.52	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.52	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:19*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:19*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm7.kmldo.local
	IPv4-адрес	10.1.6.52
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.53

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:11*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.53	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.53	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:20*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:20*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.0*			

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm11.kmldo.local
	IPv4-адрес	10.1.6.53
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.54

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:03*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.54	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.54	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:27*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:27*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm8.kmldo.local
	IPv4-адрес	10.1.6.54
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.55

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:03*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.55	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.55	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:23*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:23*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm9.kmldo.local
	IPv4-адрес	10.1.6.55
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.56

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:15:03*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.56	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.56	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:30*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:09:30*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm10.kmldo.local
	IPv4-адрес	10.1.6.56
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.57

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	regkdc-arm11.kmldo.local
	IPv4-адрес	10.1.6.57

Хост: 10.1.6.58

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.58

Хост: 10.1.6.59

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	priem-medchast.kmldo.local
	IPv4-адрес	10.1.6.59

Хост: 10.1.6.60

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.60

Хост: 10.1.6.61

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.61

Хост: 10.1.6.62

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	oker-k220a-2.kmldo.local
	IPv4-адрес	10.1.6.62

Хост: 10.1.6.63

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.63

Хост: 10.1.6.64

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:11:56*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.64

Хост: 10.1.6.65

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:43*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.65	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.65	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [12]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
21	tcp	Информация	ftp	
Метод определения	*Статистика*			
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:08:35*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
445		tcp	Средний	microsoft-ds	
Метод определения	*Статистика*				
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*			
Системное время хоста через SMB	*Дата*	*2024-05-31T09:08:35*			
	Дата запуска	*N/A*			
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*			
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
1720		tcp	Информация	h323q931	
Метод определения	*Статистика*				
2000		tcp	Информация	cisco-sccp	
Метод определения	*Статистика*				
4899		tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*				
Продукты	*cpe:/a:famatech:radmin:3.X*				
Дополнительно	*Radmin Authentication*				
5000		tcp	Информация	upnp	
Метод определения	*Статистика*				
5001		tcp	Информация	commplex-link	
Метод определения	*Статистика*				
5002		tcp	Информация	rfe	
Метод определения	*Статистика*				

5060	tcp	Информация	sip	
Метод определения	*Статистика*			
5100	tcp	Информация	admd	
Метод определения	*Статистика*			

Информация о хосте

Общая информация	DNS-имя	248eskop-plat-2.kmldo.local
	IPv4-адрес	10.1.6.65
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.66

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:43*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.66	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.66	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [10]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
21	tcp	Информация	ftp	
Метод определения	*Статистика*			
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:02:52*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
445		tcp	Средний	microsoft-ds	
Метод определения	*Статистика*				
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*			
Системное время хоста через SMB	*Дата*	*2024-05-31T09:02:52*			
	Дата запуска	*N/A*			
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*			
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
1720		tcp	Информация	h323q931	
Метод определения	*Статистика*				
2000		tcp	Информация	cisco-sccp	
Метод определения	*Статистика*				
4899		tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*				
Продукты	*cpe:/a:famatech:radmin:3.X*				
Дополнительно	*Radmin Authentication*				
5000		tcp	Информация	upnp	
Метод определения	*Статистика*				
5060		tcp	Информация	sip	
Метод определения	*Статистика*				
5100		tcp	Информация	admd	
Метод определения	*Статистика*				

Информация о хосте

Общая информация	DNS-имя	248eskop-plat-3.kmldo.local
	IPv4-адрес	10.1.6.66
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.67

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:44*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.67	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.67	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:26*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:26*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	s-ednoralyk.kmldo.local
	IPv4-адрес	10.1.6.67
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.68

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:44*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.68	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.68	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:25*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:25*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	a-vlasova.kmldo.local
	IPv4-адрес	10.1.6.68
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.69

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.69

Хост: 10.1.6.70

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	kdc-reg-arm6.kmldo.local
	IPv4-адрес	10.1.6.70

Хост: 10.1.6.71

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.71

Хост: 10.1.6.72

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.72

Хост: 10.1.6.73

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	temp-gin-arm1.kmldo.local
	IPv4-адрес	10.1.6.73

Хост: 10.1.6.74

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	temp-gin-arm2.kmldo.local
	IPv4-адрес	10.1.6.74

Хост: 10.1.6.75

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:44*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.75	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.75	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:27*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:27*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	jk5-dv-k3.kmldo.local
	IPv4-адрес	10.1.6.75
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.76

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:44*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.76	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.76	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:28*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:28*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	ras1.kmldo.local
	IPv4-адрес	10.1.6.76
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.77

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.77

Хост: 10.1.6.78

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.78

Хост: 10.1.6.79

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.79

Хост: 10.1.6.80

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:45*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.80	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.80	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:28*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:28*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	162endo-zav-otd.kmldo.local
	IPv4-адрес	10.1.6.80
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.81

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.81

Хост: 10.1.6.82

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.82

Хост: 10.1.6.83

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.83

Хост: 10.1.6.84

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.84

Хост: 10.1.6.85

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.85

Хост: 10.1.6.86

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.86

Хост: 10.1.6.87

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.87

Хост: 10.1.6.88

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.88

Хост: 10.1.6.89

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.89

Хост: 10.1.6.90

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.90

Хост: 10.1.6.91

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.91

Хост: 10.1.6.92

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.92

Хост: 10.1.6.93

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.93

Хост: 10.1.6.94

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.94

Хост: 10.1.6.95

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.95

Хост: 10.1.6.96

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.96

Хост: 10.1.6.97

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.97

Хост: 10.1.6.98

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:54*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.98

Хост: 10.1.6.99

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.99

Хост: 10.1.6.100

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.100

Хост: 10.1.6.101

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.101

Хост: 10.1.6.102

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.102

Хост: 10.1.6.103

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.103

Хост: 10.1.6.104

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.104

Хост: 10.1.6.105

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.105

Хост: 10.1.6.106

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.106

Хост: 10.1.6.107

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.107

Хост: 10.1.6.108

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.108

Хост: 10.1.6.109

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.109

Хост: 10.1.6.110

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.110

Хост: 10.1.6.111

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:45*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [12]

Хост	CVE	Риск	Описание
10.1.6.111	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.111	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.111	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.111\IPC$ (READ)*		
10.1.6.111	CVE-2017-0143	Высокий	SMBv1 сервер в Microsoft Windows Vista SP2; Windows Server 2008 SP2 и R2 SP1; Windows 7 SP1; Windows 8.1; Windows...
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) (smb-vuln-ms17-010)*		
10.1.6.111	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.111	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.111	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.111\IPC$ (READ)*		

10.1.6.111	CVE-2017-0143	Высокий	SMBv1 сервер в Microsoft Windows Vista SP2; Windows Server 2008 SP2 и R2 SP1; Windows 7 SP1; Windows 8.1; Windows...
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) (smb-vuln-ms17-010)*		
10.1.6.111	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.111	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.111	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*start date: 2024-05-31T04:53:02 (smb2-time)*		
10.1.6.111	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*start date: 2024-05-31T04:53:02 (smb2-time)*		

Инвентаризация

Продукты [8]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*2.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:14:20*		
	Дата запуска	*2024-05-31T04:53:02*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*<blank>*		
	Уровень аутентификации	*user*		

	Challenge-Response протокол	*supported*			
	Подпись сообщений	*disabled*			
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
445	tcp	Высокий	microsoft-ds	workgroup: KMLDO	
Метод определения	*Probed*				
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*				
Дополнительно	*workgroup: KMLDO*				
Параметры SMB2	*2.1*	*Message signing enabled but not required*			
Системное время хоста через SMB	*Дата*	*2024-05-31T09:14:20*			
	Дата запуска	*2024-05-31T04:53:02*			
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*			
Параметры SMB	*Используемый аккаунт*	*<blank>*			
	Уровень аутентификации	*user*			
	Challenge-Response протокол	*supported*			
	Подпись сообщений	*disabled*			
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
4899	tcp	Информация	radmin	Radmin Authentication	
Метод определения	*Probed*				
Продукты	*cpe:/a:famatech:radmin:3.X*				
Дополнительно	*Radmin Authentication*				
49152	tcp	Информация	msrpc		
Метод определения	*Probed*				
Продукты	*cpe:/a:microsoft:windows_rpc:*				
49153	tcp	Информация	msrpc		
Метод определения	*Probed*				
Продукты	*cpe:/a:microsoft:windows_rpc:*				
49154	tcp	Информация	msrpc		
Метод определения	*Probed*				
Продукты	*cpe:/a:microsoft:windows_rpc:*				
49165	tcp	Информация	msrpc		
Метод определения	*Probed*				
Продукты	*cpe:/a:microsoft:windows_rpc:*				

Информация о хосте

Общая информация	DNS-имя	SK-KONT-APT-11 | sk-kont-apt-11.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-APT-11.kmldo.local
	IPv4-адрес	10.1.6.111
	lanmanager	Windows 7 Professional 6.1
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-APT-11\x00
	Системное время	2024-05-31T12:14:20+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.111\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.111\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.111\IPC$
	Анонимный доступ	READ
Общая папка	Имя	\\10.1.6.111\PRINT$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.111\USERS
	Анонимный доступ	<none>

Хост: 10.1.6.112

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:25:49*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [8]

Хост	CVE	Риск	Описание
10.1.6.112	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.112	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.112	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.112\IPC$ (READ)*		
10.1.6.112	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.112	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.112	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.112\IPC$ (READ)*		
10.1.6.112	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.112	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

Инвентаризация

Продукты [9]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:30*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*guest*		
	Уровень аутентификации	*user*		
	Challenge-Response протокол	*supported*		
	Подпись сообщений	*disabled*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Высокий	microsoft-ds	workgroup: KMLDO
Метод определения	*Probed*			
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*			
Дополнительно	*workgroup: KMLDO*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:30*		
	Дата запуска	*N/A*		

Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

2047	tcp	Информация	dls	
Метод определения	*Статистика*			
4899	tcp	Информация	radmin	
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.0*			
5000	tcp	Информация	upnp	
Метод определения	*Статистика*			
5001	tcp	Информация	commplex-link	
Метод определения	*Статистика*			
5002	tcp	Информация	rfe	
Метод определения	*Статистика*			
5100	tcp	Информация	admd	
Метод определения	*Статистика*			

Информация о хосте

Общая информация	DNS-имя	SK-KONT-9 | sk-kont-9.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-9.kmldo.local
	IPv4-адрес	10.1.6.112
	lanmanager	Windows 10 Enterprise LTSC 2019 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-9\x00
	Системное время	2024-05-31T12:15:30+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Общая папка	Имя	\\10.1.6.112\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.112\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.112\E$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.112\IPC$
	Анонимный доступ	READ

Хост: 10.1.6.113

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-5.kmldo.local
	IPv4-адрес	10.1.6.113

Хост: 10.1.6.114

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	ok-naniyanc.kmldo.local
	IPv4-адрес	10.1.6.114

Хост: 10.1.6.115

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.115

Хост: 10.1.6.116

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-2.kmldo.local
	IPv4-адрес	10.1.6.116

Хост: 10.1.6.117

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:45*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [8]

Хост	CVE	Риск	Описание
10.1.6.117	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.117	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.117	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.117\IPC$ (READ)*		
10.1.6.117	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.117	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.117	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.117\IPC$ (READ)*		
10.1.6.117	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.117	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:31*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*guest*		
	Уровень аутентификации	*user*		
	Challenge-Response протокол	*supported*		
	Подпись сообщений	*disabled*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Высокий	microsoft-ds	workgroup: KMLDO
Метод определения	*Probed*			
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*			
Дополнительно	*workgroup: KMLDO*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:31*		
	Дата запуска	*N/A*		

Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	SK-KONT-APT-7 | sk-kont-apt-7.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-APT-7.kmldo.local
	IPv4-адрес	10.1.6.117
	lanmanager	Windows 10 Pro 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-APT-7\x00
	Системное время	2024-05-31T12:15:31+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.117\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.117\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.117\IPC$
	Анонимный доступ	READ

Хост: 10.1.6.118

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-apt-5.kmldo.local
	IPv4-адрес	10.1.6.118

Хост: 10.1.6.119

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.119

Хост: 10.1.6.120

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:46*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [8]

Хост	CVE	Риск	Описание
10.1.6.120	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.120	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.120	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.120\IPC$ (READ)*		
10.1.6.120	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.120	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.120	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.120\IPC$ (READ)*		
10.1.6.120	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.120	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:32*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*guest*		
	Уровень аутентификации	*user*		
	Challenge-Response протокол	*supported*		
	Подпись сообщений	*disabled*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Высокий	microsoft-ds	workgroup: KMLDO
Метод определения	*Probed*			
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*			
Дополнительно	*workgroup: KMLDO*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:32*		
	Дата запуска	*N/A*		

Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	SK-KONT-6 | sk-kont-6.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-6.kmldo.local
	IPv4-адрес	10.1.6.120
	lanmanager	Windows 10 Enterprise LTSC 2019 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-6\x00
	Системное время	2024-05-31T12:15:32+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.120\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.120\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.120\IPC$
	Анонимный доступ	READ
Общая папка	Имя	\\10.1.6.120\PRINT$

	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.120\USERS
	Анонимный доступ	<none>

Хост: 10.1.6.121

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.121

Хост: 10.1.6.122

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.122

Хост: 10.1.6.123

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:46*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [10]

Хост	CVE	Риск	Описание
10.1.6.123	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.123	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.123	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.123\IPC$ (READ)*		
10.1.6.123	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.123	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.123	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.123\IPC$ (READ)*		
10.1.6.123	ALTXID-324288	Высокий	Имя субъекта сертификата не соответствуют доменному имени узла.В домене установлен сертификат, который был выдан...
Продукты			
Порт	*7070 (tcp)*		
Точность	*Высокая*		
Детализация	*subject:commonName|X509v3 Subject Alternative Name: anydesk client hostNames:sk-kont-apt-1.kmldo.local|SK-KONT-APT-1*		
10.1.6.123	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*
Порт	*139 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

10.1.6.123	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

10.1.6.123	ALTXID-324287	Средний	Некорректная цепочка сертификатов (самоподписанный сертификат). Не рекомендуется использовать самоподписанный сертификат.

Продукты	
Порт	*7070 (tcp)*
Точность	*Высокая*
Детализация	*subject:commonName: AnyDesk Clientissuer:commonName: AnyDesk Client*

Инвентаризация

Продукты [13]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
21	tcp	Информация	ftp	
Метод определения	*Статистика*			
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:33*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*guest*		
	Уровень аутентификации	*user*		
	Challenge-Response протокол	*supported*		
	Подпись сообщений	*disabled*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
445		tcp	Высокий	microsoft-ds	workgroup: KMLDO
Метод определения	*Probed*				
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*				
Дополнительно	*workgroup: KMLDO*				
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*			
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:33*			
	Дата запуска	*N/A*			
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*			
Параметры SMB	*Используемый аккаунт*	*guest*			
	Уровень аутентификации	*user*			
	Challenge-Response протокол	*supported*			
	Подпись сообщений	*disabled*			
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*				
1720		tcp	Информация	h323q931	
Метод определения	*Статистика*				
2000		tcp	Информация	cisco-sccp	
Метод определения	*Статистика*				
4899		tcp	Информация	radmin	Radmin Authentication

Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			
5000	tcp	Информация	upnp	
Метод определения	*Статистика*			
5001	tcp	Информация	commplex-link	
Метод определения	*Статистика*			
5002	tcp	Информация	rfe	
Метод определения	*Статистика*			
5060	tcp	Информация	sip	
Метод определения	*Статистика*			
5100	tcp	Информация	admd	
Метод определения	*Статистика*			
7070	tcp	Высокий	realserver	
Метод определения	*Статистика*			

SSL сертификат	*Начало действия*	*2022-12-02T08:11:19*
	Конец действия	*2072-11-19T08:11:19*
	Субъект - имя	*AnyDesk Client*
	Издатель - имя	*AnyDesk Client*
	Публичный ключ - тип	*rsa*
	Публичный ключ - разрядность	*2048*
	Публичный ключ - модуль	*B3AC4F7C49D0D14760BAB2182C0E5A8F58B6EB9681E685735A0BD6ACA332A75A94A4C6A292C0C6687F40579F DD2DE42DC2D40EB084448A2E6BF210102ADCF239385F7FDFC37C6C0775E4B7561A9BE06E5DF5FE27A7DA8C620 FE09458274F9EBFA78A5F079510AD9CC42BF0407ADEEF9D70754A18C55E7188CBF6875433A5D26A977A487689 C3A0B7B8119FE64C4FF29F1EE6C84393EFE09DE116EC109C461010DD42340622AB104F3AB82DFAB510ABF3183B 8A884659B64E6B7380BBFD8856D2CD79757CC68DFDF9AE1927E345DBCFED68372B02F718244F6987F6CEBC780 A47BB47E8E74B0474E188C571C545B895DF42D8CAAA93DA58E210A067CA93D90487*
	Публичный ключ - экспонента	*65537*
	Алгоритм шифрования	*sha256WithRSAEncryption*
	md5	*522b244089f8cd5d17ef9aaa603e3519*
	sha1	*069e63ccad3633d785cdec430604bea8e11ebf4b*
	pem	*-----BEGIN CERTIFICATE----- MIICqDCCAZACAQEwDQYJKoZIhvcNAQELBQAwGTEXMBUGA1UEAwwOQW55RGVzayBD bGllbnQwIBcNMjIxMjAyMDgxMTE5WhgPMjA3MjExMTkwODExMTlaMBkxFzAVBgNV BAMMDkFueURlc2sgQ2xpZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC AQEAs6xPfEnQ0UdgurIYLA5aj1i265aB5oVzWgvWrKMyp1qUpMaiksDGaH9AV5/d LeQtwtQOsIREii5r8hAQKtzyOThff9/DfGwHdeS3Vhqb4G5d9f4np9qMYg/glFgn T56/p4pfB5UQrZzEK/BAet7vnXB1ShjFXnGIy/aHVDOl0mqXekh2icOgt7gRn+ZM T/KfHubIQ5Pv4J3hFuwQnEYQEN1CNAYiqxBPOrgt+rUQq/MYO4qIRlm2TmtzgLv9 iFbSzXl1fMaN/fmuGSfjRdvP7Wg3KwL3GCRPaYf2zrx4Cke7R+jnSwR04YjFccVF uJXfQtjKqpPaWOIQoGfKk9kEhwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAvT0nh mquvuioAfb+3PSzUz2ZN3xjCdgSSGViM9NbhS0UxG7eHBv7FFqtf6p6KS6pjltZT /S+Ds0PjhrD+fy7fDgfs359JxCsD+2eF3BzORlMgxppzh2B6XX8kzIxotWIHLDou m5Prsmm7qJLoZlf/ur3TSTcLUGQh2QSsUMFqzKikU9PxgudNsZKnjQYL+Ml5BVfb AtdncBZF49b2gMNzVEV7vKvPnmtX3xLD+mypvi5E31xYbMeDxkIqQUWOeuh8piMK +RQkKOTZHk2iqglbKj/XSniWoXCE8uMuAsvxXmQNjnU7qWPu2e1drliilSfciZCt qRKg4gpgX8BQ316r -----END CERTIFICATE-----*

Информация о хосте

Общая информация	DNS-имя	SK-KONT-APT-1 | sk-kont-apt-1.kmldo.local
	Домен	kmldo.local

	FQDN	SK-KONT-APT-1.kmldo.local
	IPv4-адрес	10.1.6.123
	lanmanager	Windows 10 Pro 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-APT-1\x00
	Системное время	2024-05-31T12:15:32+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.123\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.123\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.123\IPC$
	Анонимный доступ	READ
Общая папка	Имя	\\10.1.6.123\PRINT$
	Анонимный доступ	<none>

Хост: 10.1.6.124

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:31*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [10]

Хост	CVE	Риск	Описание
10.1.6.124	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.124	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.124	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.124\IPC$ (READ)*		
10.1.6.124	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_pro_19042_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.124	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_pro_19042_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.124	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_pro_19042_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.124\IPC$ (READ)*		
10.1.6.124	ALTXID-324288	Высокий	Имя субъекта сертификата не соответствуют доменному имени узла.В домене установлен сертификат, который был выдан...
Продукты			
Порт	*7070 (tcp)*		
Точность	*Высокая*		
Детализация	*subject:commonName|X509v3 Subject Alternative Name: anydesk client hostNames:sk-kont-3.kmldo.local|SK-KONT-3*		
10.1.6.124	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*
Порт	*139 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

10.1.6.124	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_pro_19042_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

10.1.6.124	ALTXID-324287	Средний	Некорректная цепочка сертификатов (самоподписанный сертификат). Не рекомендуется использовать самоподписанный сертификат.

Продукты	
Порт	*7070 (tcp)*
Точность	*Высокая*
Детализация	*subject:commonName: AnyDesk Clientissuer:commonName: AnyDesk Client*

Инвентаризация

Продукты [16]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
21	tcp	Информация	ftp	
Метод определения	*Статистика*			
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:33*		
	Дата запуска	*N/A*		
Файлы SMB	*\\10.1.6.124 \Users\.*	*2019-12-07T09:03:44 | <DIR>*		
	\\10.1.6.124 \Users\..	*2019-12-07T09:03:44 | <DIR>*		
	\\10.1.6.124 \Users\Public	*2019-12-07T09:14:52 | <DIR>*		
	\\10.1.6.124 \Users\Public\Documents	*2018-09-15T07:33:50 | <DIR>*		
	\\10.1.6.124 \Users\Public\Downloads	*2018-09-15T07:33:50 | <DIR>*		
	\\10.1.6.124 \Users\Public\Music	*2018-09-15T07:33:50 | <DIR>*		
	\\10.1.6.124 \Users\Public\ntuser.dat	*2023-10-26T10:01:55 | 8192*		
	\\10.1.6.124 \Users\Public\Pictures	*2018-09-15T07:33:50 | <DIR>*		

	\\10.1.6.124\Users\Public\user Path	*2019-12-20T07:04:47 | 38*
	\\10.1.6.124\Users\Public\Videos	*2018-09-15T07:33:50 | <DIR>*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

445	tcp	Высокий	microsoft-ds	workgroup: KMLDO

Метод определения	*Probed*	
Продукты	*cpe:/a::windows_10_pro_19042_microsoft-ds:*	
Дополнительно	*workgroup: KMLDO*	
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:33*
	Дата запуска	*N/A*
Файлы SMB	*\\10.1.6.124\Users\.*	*2019-12-07T09:03:44 | <DIR>*
	\\10.1.6.124\Users\..	*2019-12-07T09:03:44 | <DIR>*
	\\10.1.6.124\Users\Public	*2019-12-07T09:14:52 | <DIR>*
	\\10.1.6.124\Users\Public\Documents	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.124\Users\Public\Downloads	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.124\Users\Public\Music	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.124\Users\Public\ntuser.dat	*2023-10-26T10:01:55 | 8192*

	\\10.1.6.124\Users\Public\Pictures	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.124\Users\Public\user Path	*2019-12-20T07:04:47 | 38*
	\\10.1.6.124\Users\Public\Videos	*2018-09-15T07:33:50 | <DIR>*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

554	tcp	Информация	rtsp	
Метод определения	*Статистика*			
1720	tcp	Информация	h323q931	
Метод определения	*Статистика*			
2000	tcp	Информация	cisco-sccp	
Метод определения	*Статистика*			
2869	tcp	Информация	http	SSDP/UPnP
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:httpapi_httpd:2.0*			
Дополнительно	*SSDP/UPnP*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			
5000	tcp	Информация	upnp	
Метод определения	*Статистика*			
5001	tcp	Информация	commplex-link	
Метод определения	*Статистика*			

5002		tcp	Информация	rfe	
Метод определения	*Статистика*				
5060		tcp	Информация	sip	
Метод определения	*Статистика*				
5100		tcp	Информация	admd	
Метод определения	*Статистика*				
7070		tcp	Высокий	realserver	
Метод определения	*Статистика*				
SSL сертификат	*Начало действия*	*2022-03-29T06:03:51*			
	Конец действия	*2072-03-16T06:03:51*			
	Субъект - имя	*AnyDesk Client*			
	Издатель - имя	*AnyDesk Client*			
	Публичный ключ - тип	*rsa*			
	Публичный ключ - разрядность	*2048*			
	Публичный ключ - модуль	*C8E0B68A7F3CDCF1293B3EBAD0F36252BE67DD07C95BD97CF052FCEA804E17C913C96EED156834DF1551ABFF400118DEDBB0CB3E8958871D1B9B978E0FDB01B4C46D3F843F1A46C622CBF67FD00E6154F94721DA1BDE8574F3F4EA56A51CADD8ED9D5DC0ED773AD46F0F31EA4EF7461DC8179A0A52BE203B73DFC0293DD855643FAEB772E82AA3A5206119E06F77BDF8E48891D3194D403E0FA3A969BFAB4785C822BD0FEF0E45BA28BD7C629EA4F32B79596772F9C9825E1C328995DC287225EBC4FA4E0491DB4CA064CCAF104502ABDB67D7C5961A44B3CDD3D9F85D2FFB87B0C18EADB8C08886D479B159E2446EBBDB54F77F4BF7FD9F76C9CD3A9972D28F*			
	Публичный ключ - экспонента	*65537*			
	Алгоритм шифрования	*sha256WithRSAEncryption*			
	md5	*9f079954fc2bed8c16b4511bd4be0198*			
	sha1	*40bcca621b95fbce59deaffded5dd3b222f05b51*			
	pem	*-----BEGIN CERTIFICATE----- MIICqDCCAZACAQEwDQYJKoZIhvcNAQELBQAwGTEXMBUGA1UEAwwOQW55RGVzayBDbGllbnQwIBcNMjIwMzI5MDYwMzUxWhgPMjA3MjAzMTYwNjAzNTFaMBkxFzAVBgNVBAMMDkFueURlc2sgQ2xpZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyOC2in883PEpOz660PNiUr5n3QfJW9l88FL86oBOF8kTyW7tFWg03xVRq/9AARje27DLPolYhx0bm5eOD9sBtMRtP4Q/GkbGIsv2f9AOYVT5RyHaG96FdPP06lalHK3Y7Z1dwO13OtRvDzHqTvdGHcgXmgpSviA7c9/AKT3YVWQ/rrdy6CqjpSBhGeBvd7345IiR0xlNQD4Po6lpv6tHhcgivQ/vDkW6KL18Yp6k8yt5WWdy+cmCXhwyiZXcKHIl68T6TgSR20ygZMyvEEUCq9tn18WWGkSzzdPZ+F0v+4ewwY6tuMClhtR5sVniRG6721T3f0v3/Z92yc06mXLSjwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCa3PVD19W68heWvnEOEsT/BpxIllx8Hht5eruD4Q215PD+e72Ou0BwauLoYxnXFNSCvex2FiNisWZqpipUVyApc73hUMj4Ftl4zGTV+YPogt/DxQQckjF7Paj8ZuUnQV7gDamZU8kKeWydbU5TA3QelyvObi21wB8QGlZcB4gwQhAEUo5szL0k7mimvdeDkxymrewHDbUyviy/+tyy7ac2P289jaOrOcvC+FW0aB1HKcn98epriizYcYHKMsUMbyAPinSiMq7M1ZtWkXEGwsgDdZfSH2yaj633hXn3Nbltx/rx9WBxk3q3Gtd8YzpGvm1LEgHs2p5lJMQmAG293W8V* *-----END CERTIFICATE-----*			
Шифрование	*TLSv1.2*	*TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A*			
10243		tcp	Информация	http	SSDP/UPnP
Метод определения	*Probed*				
Продукты	*cpe:/a:microsoft:httpapi_httpd:2.0*				

Дополнительно	*SSDP/UPnP*
Системное время хоста через http	*Fri, 31 May 2024 09:16:02 GMT; 0s from local time.*
Http заголовки	*Content-Type: text/html; charset=us-ascii* *Server: Microsoft-HTTPAPI/2.0* *Date: Fri, 31 May 2024 09:16:02 GMT* *Connection: close* *Content-Length: 315* *(Request type: GET)*

Информация о хосте

Общая информация	DNS-имя	SK-KONT-3 | sk-kont-3.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-3.kmldo.local
	IPv4-адрес	10.1.6.124
	lanmanager	Windows 10 Pro 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-3\x00
	Системное время	2024-05-31T12:15:33+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.124\ADMIN$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0 \xBD\xD1\x8B\xD0\xB9 Admin
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.124\C$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1 \x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1 \xD1\x89\xD0\xB8\xD0\xB9 \xD1\x80\xD0\xB5\xD1\x81\xD1 \x83\xD1\x80\xD1\x81
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.124\HP LaserJet M1530 MFP Series PCL 6
	Тип	STYPE_PRINTQ
	Комментарий	HP LaserJet M1530 MFP Series PCL 6
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ
Общая папка	Имя	\\10.1.6.124\IPC$
	Тип	STYPE_IPC_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0 \xBD\xD1\x8B\xD0\xB9 IPC
	Анонимный доступ	READ
	Доступ для текущего пользователя	READ/WRITE
Общая папка	Имя	\\10.1.6.124\NPIC7B181 (HP LaserJet M402dn)
	Тип	STYPE_PRINTQ

	Комментарий	NPIC7B181 (HP LaserJet M402dn)
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ
Общая папка	Имя	\\10.1.6.124\print$
	Тип	STYPE_DISKTREE
	Комментарий	\xD0\x94\xD1\x80\xD0\xB0\xD0\xB9\xD0\xB2\xD0\xB5\xD1\x80\xD1\x8B \xD0\xBF\xD1\x80\xD0\xB8\xD0\xBD\xD1\x82\xD0\xB5\xD1\x80\xD0\xBE\xD0\xB2
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ
Общая папка	Имя	\\10.1.6.124\Users
	Тип	STYPE_DISKTREE
	Комментарий	
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ

Хост: 10.1.6.125

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-apt-4.kmldo.local
	IPv4-адрес	10.1.6.125

Хост: 10.1.6.126

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-1.kmldo.local
	IPv4-адрес	10.1.6.126

Хост: 10.1.6.127

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:22:55*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-4.kmldo.local
	IPv4-адрес	10.1.6.127

Хост: 10.1.6.128

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:26:47*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [8]

Хост	CVE	Риск	Описание
10.1.6.128	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.128	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.128	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.128\IPC$ (READ)*		
10.1.6.128	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.128	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.128	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.128\IPC$ (READ)*		
10.1.6.128	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.128	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:34*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*guest*		
	Уровень аутентификации	*user*		
	Challenge-Response протокол	*supported*		
	Подпись сообщений	*disabled*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Высокий	microsoft-ds	workgroup: KMLDO
Метод определения	*Probed*			
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*			
Дополнительно	*workgroup: KMLDO*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:15:34*		
	Дата запуска	*N/A*		

Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

808	tcp	Информация	mc-nmf	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:.net_message_framing:*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	SK-KONT-APT-3 | konts-pilipenko.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-APT-3.kmldo.local
	IPv4-адрес	10.1.6.128
	lanmanager	Windows 10 Pro 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-APT-3\x00
	Системное время	2024-05-31T12:15:35+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.128\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.128\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.128\IPC$
	Анонимный доступ	READ

Хост: 10.1.6.129

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:30:35*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.129	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.129	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:25*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:25*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	sk-kont-apt-2.kmldo.local
	IPv4-адрес	10.1.6.129
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.130

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:17*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [8]

Хост	CVE	Риск	Описание
10.1.6.130	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.130	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.130	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.130\IPC$ (READ)*		
10.1.6.130	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.130	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.130	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.130\IPC$ (READ)*		
10.1.6.130	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.130	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:24*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*guest*		
	Уровень аутентификации	*user*		
	Challenge-Response протокол	*supported*		
	Подпись сообщений	*disabled*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Высокий	microsoft-ds	workgroup: KMLDO
Метод определения	*Probed*			
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*			
Дополнительно	*workgroup: KMLDO*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:24*		
	Дата запуска	*N/A*		

Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

4899	tcp	Информация	radmin	
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.0*			

Информация о хосте

Общая информация	DNS-имя	SK-KONT-APT-8 | sk-kont-apt-8.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-APT-8.kmldo.local
	IPv4-адрес	10.1.6.130
	lanmanager	Windows 10 Pro 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-APT-8\x00
	Системное время	2024-05-31T12:24:25+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.130\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.130\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.130\D$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.130\IPC$
	Анонимный доступ	READ
Общая папка	Имя	\\10.1.6.130\USERS
	Анонимный доступ	<none>

Хост: 10.1.6.131

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:17*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-7.kmldo.local
	IPv4-адрес	10.1.6.131

Хост: 10.1.6.132

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:17*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-apt-13.kmldo.local
	IPv4-адрес	10.1.6.132

Хост: 10.1.6.133

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:17*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	sk-kont-apt-9.kmldo.local
	IPv4-адрес	10.1.6.133

Хост: 10.1.6.134

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:30:35*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [10]

Хост	CVE	Риск	Описание
10.1.6.134	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.134	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.134	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.134\IPC$ (READ)*		
10.1.6.134	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.134	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.134	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.134\IPC$ (READ)*		
10.1.6.134	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.134	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

10.1.6.134	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...

Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*
Порт	*139 (tcp)*
Точность	*Высокая*
Детализация	*start date: 2024-05-31T04:53:52 (smb2-time)*

10.1.6.134	ALTXID-341903	Низкий	Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки...

Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*start date: 2024-05-31T04:53:52 (smb2-time)*

Инвентаризация

Продукты [10]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	

Метод определения	*Probed*
Продукты	*cpe:/a:microsoft:windows_rpc:*

139	tcp	Высокий	netbios-ssn	

Метод определения	*Probed*	
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*	
Параметры SMB2	*2.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:26*
	Дата запуска	*2024-05-31T04:53:52*
Файлы SMB	*\\10.1.6.134\Users\.*	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\..	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\Documents	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\Downloads	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\Music	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\ntuser.dat	*2019-04-24T12:36:09 | 262144*
	\\10.1.6.134\Users\Public\Pictures	*2009-07-14T03:20:08 | <DIR>*

	\\10.1.6.134\Users\Public\Recorded TV	*2011-04-12T13:37:14 | <DIR>*
	\\10.1.6.134\Users\Public\Videos	*2009-07-14T03:20:08 | <DIR>*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

445 tcp Высокий microsoft-ds workgroup: KMLDO

Метод определения	*Probed*	
Продукты	*cpe:/a::windows_7_professional_7601_service_pack_1_microsoft-ds:*	
Дополнительно	*workgroup: KMLDO*	
Параметры SMB2	*2.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:26*
	Дата запуска	*2024-05-31T04:53:52*
Файлы SMB	*\\10.1.6.134\Users\.*	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\..	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\Documents	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\Downloads	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\Music	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\ntuser.dat	*2019-04-24T12:36:09 | 262144*
	\\10.1.6.134\Users\Public\Pictures	*2009-07-14T03:20:08 | <DIR>*
	\\10.1.6.134\Users\Public\Recorded TV	*2011-04-12T13:37:14 | <DIR>*
	\\10.1.6.134\Users\Public\Videos	*2009-07-14T03:20:08 | <DIR>*

Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			
49152	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
49153	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
49154	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
49155	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
49156	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
49157	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			

Информация о хосте

Общая информация	DNS-имя	SK-KONT-APT-10 | sk-kont-apt-10.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-APT-10.kmldo.local
	IPv4-адрес	10.1.6.134
	lanmanager	Windows 7 Professional 6.1
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-APT-10\x00
	Системное время	2024-05-31T12:24:26+03:00
Операционная система	Имя	Microsoft Windows

	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.134\ADMIN$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xB9 Admin
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.134\C$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1\x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1\xD1\x89\xD0\xB8\xD0\xB9 \xD1\x80\xD0\xB5\xD1\x81\xD1\x83\xD1\x80\xD1\x81
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.134\IPC$
	Тип	STYPE_IPC_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xB9 IPC
	Анонимный доступ	READ
	Доступ для текущего пользователя	READ/WRITE
Общая папка	Имя	\\10.1.6.134\print$
	Тип	STYPE_DISKTREE
	Комментарий	\xD0\x94\xD1\x80\xD0\xB0\xD0\xB9\xD0\xB2\xD0\xB5\xD1\x80\xD1\x8B \xD0\xBF\xD1\x80\xD0\xB8\xD0\xBD\xD1\x82\xD0\xB5\xD1\x80\xD0\xBE\xD0\xB2
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ
Общая папка	Имя	\\10.1.6.134\Users
	Тип	STYPE_DISKTREE
	Комментарий	
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ

Хост: 10.1.6.135

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:30:35*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [8]

Хост	CVE	Риск	Описание
10.1.6.135	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.135	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.135	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.135\IPC$ (READ)*		
10.1.6.135	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.135	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.135	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.135\IPC$ (READ)*		
10.1.6.135	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.135	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

Инвентаризация

Продукты [5]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Высокий	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:26*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*		
Параметры SMB	*Используемый аккаунт*	*guest*		
	Уровень аутентификации	*user*		
	Challenge-Response протокол	*supported*		
	Подпись сообщений	*disabled*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Высокий	microsoft-ds	workgroup: KMLDO
Метод определения	*Probed*			
Продукты	*cpe:/a::windows_10_pro_19045_microsoft-ds:*			
Дополнительно	*workgroup: KMLDO*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:24:26*		
	Дата запуска	*N/A*		

Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

5357	tcp	Информация	http	SSDP/UPnP
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:httpapi_httpd:2.0*			
Дополнительно	*SSDP/UPnP*			
Http заголовки	*Content-Type: text/html; charset=us-ascii* *Server: Microsoft-HTTPAPI/2.0* *Date: Fri, 31 May 2024 09:25:07 GMT* *Connection: close* *Content-Length: 326* *(Request type: GET)*			

Информация о хосте

Общая информация	DNS-имя	SK-KONT-8 | sk-kont-8.kmldo.local
	Домен	kmldo.local
	FQDN	SK-KONT-8.kmldo.local
	IPv4-адрес	10.1.6.135
	lanmanager	Windows 10 Pro 6.3
	Рабочая группа	KMLDO\x00
	Сервер	SK-KONT-8\x00
	Системное время	2024-05-31T12:24:27+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Общая папка	Имя	\\10.1.6.135\ADMIN$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.135\C$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.135\IPC$
	Анонимный доступ	READ
Общая папка	Имя	\\10.1.6.135\PRINT$
	Анонимный доступ	<none>
Общая папка	Имя	\\10.1.6.135\USERS
	Анонимный доступ	<none>

Хост: 10.1.6.136

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:17*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.136

Хост: 10.1.6.137

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:17*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.137

Хост: 10.1.6.138

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.138

Хост: 10.1.6.139

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.139

Хост: 10.1.6.140

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.140

Хост: 10.1.6.141

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:30:35*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [8]

Хост	CVE	Риск	Описание
10.1.6.141	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.141	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.141	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.141\IPC$ (READ)*		
10.1.6.141	ALTXID-324283	Высокий	Отключено подписывание SMB пакетов
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*message_signing: disabled (smb-security-mode)*		
10.1.6.141	ALTXID-324284	Высокий	Обнаружен устаревший протокол SMBv1
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*NT LM 0.12 (SMBv1) [dangerous, but default] (smb-protocols)*		
10.1.6.141	ALTXID-324282	Высокий	Обнаружены общие папки с анонимным доступом
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*		
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*\\10.1.6.141\IPC$ (READ)*		
10.1.6.141	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.141	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно

Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*
Порт	*445 (tcp)*
Точность	*Высокая*
Детализация	*Message signing enabled but not required (smb2-security-mode)*

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	

Метод определения	*Probed*	
Продукты	*cpe:/a:microsoft:windows_rpc:*	

Порт	Протокол	Риск	Имя сервиса	Дополнительно
139	tcp	Высокий	netbios-ssn	

Метод определения	*Probed*	
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*	
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T09:19:51*
	Дата запуска	*N/A*
Файлы SMB	*\\10.1.6.141 \print$\.*	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\..	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\color	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\IA64	*2019-04-18T06:52:12 | <DIR>*
	\\10.1.6.141 \print$\W32X86	*2019-04-18T06:52:12 | <DIR>*
	\\10.1.6.141 \print$\W32X86\3	*2019-04-18T06:52:13 | <DIR>*
	\\10.1.6.141 \print$\W32X86 \PCC	*2019-04-18T06:52:13 | <DIR>*
	\\10.1.6.141 \print$\x64	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\x64\3	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\x64\PCC	*2019-04-18T06:52:12 | <DIR>*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*	

445 tcp Высокий microsoft-ds workgroup: WORKGROUP

Метод определения	*Probed*	
Продукты	*cpe:/a::windows_10_enterprise_ltsc_2019_17763_microsoft-ds:*	
Дополнительно	*workgroup: WORKGROUP*	
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*
Системное время хоста через SMB	*Дата*	*2024-05-31T09:19:51*
	Дата запуска	*N/A*
Файлы SMB	*\\10.1.6.141 \print$\.*	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\..	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\color	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\IA64	*2019-04-18T06:52:12 | <DIR>*
	\\10.1.6.141 \print$\W32X86	*2019-04-18T06:52:12 | <DIR>*
	\\10.1.6.141 \print$\W32X86\3	*2019-04-18T06:52:13 | <DIR>*
	\\10.1.6.141 \print$\W32X86 \PCC	*2019-04-18T06:52:13 | <DIR>*
	\\10.1.6.141 \print$\x64	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\x64\3	*2018-09-15T07:33:50 | <DIR>*
	\\10.1.6.141 \print$\x64\PCC	*2019-04-18T06:52:12 | <DIR>*
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1 | NT LM 0.12 (SMBv1) [dangerous, but default]*
Параметры SMB	*Используемый аккаунт*	*guest*
	Уровень аутентификации	*user*
	Challenge-Response протокол	*supported*
	Подпись сообщений	*disabled*

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*

4899	tcp	Информация	radmin	Radmin Authentication

Метод определения	*Probed*
Продукты	*cpe:/a:famatech:radmin:3.X*
Дополнительно	*Radmin Authentication*

Информация о хосте

Общая информация	DNS-имя	PAPAZYANPC
	Домен	PapazyanPC
	FQDN	PapazyanPC
	IPv4-адрес	10.1.6.141
	lanmanager	Windows 10 Enterprise LTSC 2019 6.3
	Рабочая группа	WORKGROUP\x00
	Сервер	PAPAZYANPC\x00
	Системное время	2024-05-31T12:19:51+03:00
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows
Общая папка	Имя	\\10.1.6.141\ADMIN$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0 \xBD\xD1\x8B\xD0\xB9 Admin
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.141\C$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1 \x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1 \xD1\x89\xD0\xB8\xD0\xB9 \xD1\x80\xD0\xB5\xD1\x81\xD1 \x83\xD1\x80\xD1\x81
	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.141\D$
	Тип	STYPE_DISKTREE_HIDDEN
	Комментарий	\xD0\xA1\xD1\x82\xD0\xB0\xD0\xBD\xD0\xB4\xD0\xB0\xD1 \x80\xD1\x82\xD0\xBD\xD1\x8B\xD0\xB9 \xD0\xBE\xD0\xB1 \xD1\x89\xD0\xB8\xD0\xB9 \xD1\x80\xD0\xB5\xD1\x81\xD1 \x83\xD1\x80\xD1\x81

	Анонимный доступ	<none>
	Доступ для текущего пользователя	<none>
Общая папка	Имя	\\10.1.6.141\IPC$
	Тип	STYPE_IPC_HIDDEN
	Комментарий	\xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xB9 IPC
	Анонимный доступ	READ
	Доступ для текущего пользователя	READ/WRITE
Общая папка	Имя	\\10.1.6.141\print$
	Тип	STYPE_DISKTREE
	Комментарий	\xD0\x94\xD1\x80\xD0\xB0\xD0\xB9\xD0\xB2\xD0\xB5\xD1\x80\xD1\x8B \xD0\xBF\xD1\x80\xD0\xB8\xD0\xBD\xD1\x82\xD0\xB5\xD1\x80\xD0\xBE\xD0\xB2
	Анонимный доступ	<none>
	Доступ для текущего пользователя	READ

Хост: 10.1.6.142

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.142

Хост: 10.1.6.143

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	kdc-reng-k212-5.kmldo.local
	IPv4-адрес	10.1.6.143

Хост: 10.1.6.144

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	rg-laborant2.kmldo.local
	IPv4-адрес	10.1.6.144

Хост: 10.1.6.145

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	rg-laborant3.kmldo.local
	IPv4-адрес	10.1.6.145

Хост: 10.1.6.146

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	rg-laborant4.kmldo.local
	IPv4-адрес	10.1.6.146

Хост: 10.1.6.147

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.147

Хост: 10.1.6.148

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.148

Хост: 10.1.6.149

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.149

Хост: 10.1.6.150

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.150

Хост: 10.1.6.151

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.151

Хост: 10.1.6.152

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.152

Хост: 10.1.6.153

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.153

Хост: 10.1.6.154

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.154

Хост: 10.1.6.155

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.155

Хост: 10.1.6.156

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.156

Хост: 10.1.6.157

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.157

Хост: 10.1.6.158

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.158

Хост: 10.1.6.159

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.159

Хост: 10.1.6.160

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.160

Хост: 10.1.6.161

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.161

Хост: 10.1.6.162

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.162

Хост: 10.1.6.163

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.163

Хост: 10.1.6.164

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.164

Хост: 10.1.6.165

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.165

Хост: 10.1.6.166

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.166

Хост: 10.1.6.167

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.167

Хост: 10.1.6.168

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.168

Хост: 10.1.6.169

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.169

Хост: 10.1.6.170

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.170

Хост: 10.1.6.171

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.171

Хост: 10.1.6.172

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.172

Хост: 10.1.6.173

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:18*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.173

Хост: 10.1.6.174

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.174

Хост: 10.1.6.175

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.175

Хост: 10.1.6.176

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.176

Хост: 10.1.6.177

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.177

Хост: 10.1.6.178

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.178

Хост: 10.1.6.179

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.179

Хост: 10.1.6.180

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.180

Хост: 10.1.6.181

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.181

Хост: 10.1.6.182

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.182

Хост: 10.1.6.183

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.183

Хост: 10.1.6.184

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.184

Хост: 10.1.6.185

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.185

Хост: 10.1.6.186

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.186

Хост: 10.1.6.187

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.187

Хост: 10.1.6.188

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.188

Хост: 10.1.6.189

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.189

Хост: 10.1.6.190

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.190

Хост: 10.1.6.191

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.191

Хост: 10.1.6.192

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:28:19*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.192

Хост: 10.1.6.193

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:31*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.193

Хост: 10.1.6.194

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:31*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.194

Хост: 10.1.6.195

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:31*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.195

Хост: 10.1.6.196

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:31*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.196

Хост: 10.1.6.197

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.197

Хост: 10.1.6.198

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.198

Хост: 10.1.6.199

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.199

Хост: 10.1.6.200

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.200

Хост: 10.1.6.201

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.201

Хост: 10.1.6.202

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.202

Хост: 10.1.6.203

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.203

Хост: 10.1.6.204

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.204

Хост: 10.1.6.205

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.205

Хост: 10.1.6.206

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.206

Хост: 10.1.6.207

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.207

Хост: 10.1.6.208

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.208

Хост: 10.1.6.209

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.209

Хост: 10.1.6.210

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	DNS-имя	133reab-proc-1.kmldo.local
	IPv4-адрес	10.1.6.210

Хост: 10.1.6.211

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.211

Хост: 10.1.6.212

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.212

Хост: 10.1.6.213

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.213

Хост: 10.1.6.214

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.214

Хост: 10.1.6.215

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.215

Хост: 10.1.6.216

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.216

Хост: 10.1.6.217

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.217

Хост: 10.1.6.218

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.218

Хост: 10.1.6.219

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.219

Хост: 10.1.6.220

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.220

Хост: 10.1.6.221

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.221

Хост: 10.1.6.222

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.222

Хост: 10.1.6.223

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.223

Хост: 10.1.6.224

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.224

Хост: 10.1.6.225

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.225

Хост: 10.1.6.226

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.226

Хост: 10.1.6.227

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.227

Хост: 10.1.6.228

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.228

Хост: 10.1.6.229

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.229

Хост: 10.1.6.230

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.230

Хост: 10.1.6.231

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:32*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.231

Хост: 10.1.6.232

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.232

Хост: 10.1.6.233

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.233

Хост: 10.1.6.234

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.234

Хост: 10.1.6.235

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.235

Хост: 10.1.6.236

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.236

Хост: 10.1.6.237

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.237

Хост: 10.1.6.238

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.238

Хост: 10.1.6.239

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.239

Хост: 10.1.6.240

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.240

Хост: 10.1.6.241

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.241

Хост: 10.1.6.242

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.242

Хост: 10.1.6.243

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.243

Хост: 10.1.6.244

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.244

Хост: 10.1.6.245

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.245

Хост: 10.1.6.246

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.246

Хост: 10.1.6.247

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.247

Хост: 10.1.6.248

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.248

Хост: 10.1.6.249

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.249

Хост: 10.1.6.250

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.250

Хост: 10.1.6.251

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:30:46*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости [2]

Хост	CVE	Риск	Описание
10.1.6.251	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*		
Порт	*139 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		
10.1.6.251	ALTXID-324281	Средний	Подписывание SMB2 пакетов включено, но не обязательно
Продукты			
Порт	*445 (tcp)*		
Точность	*Высокая*		
Детализация	*Message signing enabled but not required (smb2-security-mode)*		

Инвентаризация

Продукты [4]

Порт	Протокол	Риск	Имя сервиса	Дополнительно
135	tcp	Информация	msrpc	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_rpc:*			
139	tcp	Средний	netbios-ssn	
Метод определения	*Probed*			
Продукты	*cpe:/a:microsoft:windows_netbios-ssn:*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:27:18*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		

smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
445	tcp	Средний	microsoft-ds	
Метод определения	*Статистика*			
Параметры SMB2	*3.1.1*	*Message signing enabled but not required*		
Системное время хоста через SMB	*Дата*	*2024-05-31T09:27:18*		
	Дата запуска	*N/A*		
Поддерживаемые SMB протоколы	*Диалекты*	*2.0.2 | 2.1 | 3.0 | 3.0.2 | 3.1.1*		
smb2 перечень возможностей	*2.0.2:* *Distributed File System* *2.1:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0:* *Distributed File System* *Leasing* *Multi-credit operations* *3.0.2:* *Distributed File System* *Leasing* *Multi-credit operations* *3.1.1:* *Distributed File System* *Leasing* *Multi-credit operations*			
4899	tcp	Информация	radmin	Radmin Authentication
Метод определения	*Probed*			
Продукты	*cpe:/a:famatech:radmin:3.X*			
Дополнительно	*Radmin Authentication*			

Информация о хосте

Общая информация	DNS-имя	zam-keiom.kmldo.local
	IPv4-адрес	10.1.6.251
Операционная система	Имя	Microsoft Windows
	cpe	cpe:/o:microsoft:windows

Хост: 10.1.6.252

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.252

Хост: 10.1.6.253

Начало/завершение сканирования	*31.05.2024 12:06:51 / 31.05.2024 12:27:33*
Типы сканирования, включённые в отчёт	*Сканирование портов, Поиск уязвимостей*
Точность для отображения уязвимостей	*Средняя и высокая*

Поиск уязвимостей

Уязвимости не обнаружены

Инвентаризация

Информация о хосте

Общая информация	IPv4-адрес	10.1.6.253

Список уязвимостей

Уязвимость Риск: Критический

CVE-2022-2068

Описание

Уязвимость в OpenSSL 3.0.0, 3.0.1, 3.0.2, 3.0.3, 1.1.1 до 1.1.1o, и 1.0.2 до 1.0.2ze позволяет злоумышленнику выполнить произвольные команды.

Ссылки

CVE-2022-2068

CVSSv2: Базовая оценка 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-78
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2068
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=2c9c35870601b4a44d86ddbf512b38df38285cfa
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=9639817dac8bbbaa64d09efad7464ccc405527c7
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=7a9c027159fe9e1bbc2cd38a8a2914bff0d5abd9
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6WZZBKUHQFGSKGNXXKICSRPL7AMVW5M5/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/VCMNWKERPBKOEBNL7CLTTX3ZZCZLH7XA/

CONFIRM

https://www.openssl.org/news/secadv/20220621.txt

CONFIRM

https://security.netapp.com/advisory/ntap-20220707-0008/

CONFIRM

https://cert-portal.siemens.com/productcert/pdf/ssa-332410.pdf

DEBIAN

https://www.debian.org/security/2022/dsa-5169

Уязвимость Риск: Высокий

CVE-2022-22720

Описание

Проникновение HTTP-запроса (HRS) в Apache HTTP Server 2.4.52 и ниже.

Ссылки

CVE-2022-22720

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RGWILBORT67SHMSLYSQZG2NMXGCMPUZO/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Z7H26WJ6TPKNWV3QKY4BHKUKQVUTZJTD/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/X73C35MMMZGBVPQQCH7LQZUMYZNQA5FO/

CONFIRM

https://security.netapp.com/advisory/ntap-20220321-0001/

CONFIRM

https://support.apple.com/kb/HT213256

CONFIRM

https://support.apple.com/kb/HT213257

CONFIRM

https://support.apple.com/kb/HT213255

FULLDISC

http://seclists.org/fulldisclosure/2022/May/38

FULLDISC

http://seclists.org/fulldisclosure/2022/May/33

FULLDISC

http://seclists.org/fulldisclosure/2022/May/35

GENTOO

https://security.gentoo.org/glsa/202208-20

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MISC

https://www.oracle.com/security-alerts/cpuapr2022.html

MLIST

http://www.openwall.com/lists/oss-security/2022/03/14/3

MLIST

https://lists.debian.org/debian-lts-announce/2022/03/msg00033.html

N/A

https://www.oracle.com/security-alerts/cpujul2022.html

Уязвимость Риск: Высокий

CVE-2021-44790

Описание

Переполнение буфера в mod_lua в Apache HTTP Server версии с 2.4 до 2.4.51.

Ссылки

CVE-2021-44790

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-787

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44790

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/BFSWOH4X77CV7AH7C4RMHUBDWKQDL4YH/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RGWILBORT67SHMSLYSQZG2NMXGCMPUZO/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Z7H26WJ6TPKNWV3QKY4BHKUKQVUTZJTD/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/X73C35MMMZGBVPQQCH7LQZUMYZNQA5FO/

CONFIRM

https://security.netapp.com/advisory/ntap-20211224-0001/

CONFIRM

https://www.tenable.com/security/tns-2022-01

CONFIRM

https://www.tenable.com/security/tns-2022-03

CONFIRM

https://support.apple.com/kb/HT213255

CONFIRM

https://support.apple.com/kb/HT213256

CONFIRM

https://support.apple.com/kb/HT213257

DEBIAN
https://www.debian.org/security/2022/dsa-5035

FULLDISC
http://seclists.org/fulldisclosure/2022/May/38

FULLDISC
http://seclists.org/fulldisclosure/2022/May/33

FULLDISC
http://seclists.org/fulldisclosure/2022/May/35

GENTOO
https://security.gentoo.org/glsa/202208-20

MISC
http://httpd.apache.org/security/vulnerabilities_24.html

MISC
https://www.oracle.com/security-alerts/cpujan2022.html

MISC
https://www.oracle.com/security-alerts/cpuapr2022.html

MISC
http://packetstormsecurity.com/files/171631/Apache-2.4.x-Buffer-Overflow.html

MLIST
http://www.openwall.com/lists/oss-security/2021/12/20/4

Уязвимость Риск: Высокий

CVE-2022-23943

Описание

Уязвимость записи за пределами выделенной памяти в mod_sed в Apache HTTP Server позволяет злоумышленникам перезаписать память.

Ссылки

CVE-2022-23943
CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RGWILBORT67SHMSLYSQZG2NMXGCMPUZO/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Z7H26WJ6TPKNWV3QKY4BHKUKQVUTZJTD/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/X73C35MMMZGBVPQQCH7LQZUMYZNQA5FO/

CONFIRM
https://security.netapp.com/advisory/ntap-20220321-0001/

CONFIRM
https://www.tenable.com/security/tns-2022-08

CONFIRM
https://www.tenable.com/security/tns-2022-09

GENTOO
https://security.gentoo.org/glsa/202208-20

MISC
https://httpd.apache.org/security/vulnerabilities_24.html

MISC
https://www.oracle.com/security-alerts/cpuapr2022.html

MLIST
http://www.openwall.com/lists/oss-security/2022/03/14/1

MLIST

https://lists.debian.org/debian-lts-announce/2022/03/msg00033.html

Уязвимость Риск: Высокий

CVE-2022-31813

Описание

Apache HTTP Server 2.4.53 и более ранние версии могут не отправлять заголовки X-Forwarded-* на исходный сервер из-за механизма пошаговой передачи заголовка Connection на стороне клиента. Это может быть использовано для обхода IP-аутентификации на исходном сервере/приложении.

Ссылки

CVE-2022-31813

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-345
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31813
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/YPY2BLEVJWFH34AX77ZJPLD2OOBYR6ND/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7QUGG2QZWHTITMABFLVXA4DNYUOTPWYQ/

CONFIRM

https://security.netapp.com/advisory/ntap-20220624-0005/

GENTOO

https://security.gentoo.org/glsa/202208-20

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MLIST

http://www.openwall.com/lists/oss-security/2022/06/08/8

Уязвимость Риск: Высокий

ALTXID-335831

Описание

Включён режим отладки для приложений ASP.NET. Отключите режим отладки для приложений ASP.NET.

Ссылки

ALTXID-335831

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-11

Microsoft

https://docs.microsoft.com/ru-ru/troubleshoot/aspnet/disable-debugging-application

Уязвимость Риск: Высокий

CVE-2017-8923

Описание

Функция zend_string_extend в Zend/zend_string.h в PHP по 7.1.5 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) и имеет другие неизвестные воздействия.

Ссылки

CVE-2017-8923

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-787

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8923

BID

http://www.securityfocus.com/bid/98518

MISC

https://bugs.php.net/bug.php?id=74577

Уязвимость Риск: Высокий

CVE-2017-9120

Описание

PHP 7.x по 7.1.5 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (переполнение буфера и падение приложения) и имеет другие неизвестные воздействия через длинную строку из-за целочисленного переполнения в mysqli_real_escape_string.

Ссылки

CVE-2017-9120

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9120

CONFIRM

https://security.netapp.com/advisory/ntap-20181107-0003/

MISC

https://bugs.php.net/bug.php?id=74544

REDHAT

https://access.redhat.com/errata/RHSA-2019:2519

Уязвимость Риск: Высокий

ALTXID-324283

Описание

Отключено подписывание SMB пакетов

Ссылки

ALTXID-324283

CVSSv2: Базовая оценка 7.3 (AV:A/AC:M/Au:N/C:C/I:C/A:N)
CVSSv3: Базовая оценка 6.8 (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
CWE-311

MS

https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/cc731957(v=ws.11)

MS

https://support.microsoft.com/ru-ru/help/887429/overview-of-server-message-block-signing

Уязвимость Риск: Высокий

ALTXID-324284

Описание

Обнаружен устаревший протокол SMBv1

Ссылки

ALTXID-324284

CVSSv2: Базовая оценка 7.6 (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)
CVSSv3: Базовая оценка 7.5 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C)

MS

https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

MS

https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

Уязвимость Риск: Высокий

ALTXID-324282

Описание

Обнаружены общие папки с анонимным доступом

Ссылки

ALTXID-324282

CVSSv2: Базовая оценка 6.0 (AV:N/AC:H/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C)
CVSSv3: Базовая оценка 7.3 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C)
CWE-732

MS

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-shares-that-can-be-accessed-anonymously

Уязвимость Риск: Высокий

CVE-2017-0143

Описание

SMBv1 сервер в Microsoft Windows Vista SP2; Windows Server 2008 SP2 и R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold и R2; и Windows 10 Gold, 1511, и 1607; и Windows Server 2016 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированные пакеты.

Ссылки

CVE-2017-0143

CVSSv2: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSSv3: Базовая оценка 7.3 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C)
CWE-20
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

BID

http://www.securityfocus.com/bid/96703

CONFIRM

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143

CONFIRM

https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf

CONFIRM

https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf

EXPLOIT-DB

https://www.exploit-db.com/exploits/41987/

EXPLOIT-DB

https://www.exploit-db.com/exploits/41891/

EXPLOIT-DB

https://www.exploit-db.com/exploits/43970/

MISC

https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

MISC

http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

MISC

http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

SECTRACK

http://www.securitytracker.com/id/1037991

Уязвимость Риск: Высокий

ALTXID-324288

Описание

Имя субъекта сертификата не соответствуют доменному имени узла.В домене установлен сертификат, который был выдан для другого домена. Например, если сертификат выдан для домена mysite.ru, он не будет работать для домена shop.mysite.ru.

Ссылки

ALTXID-324288

CVSSv2: Базовая оценка 7.0 (AV:N/AC:H/Au:N/C:C/I:C/A:N)
CVSSv3: Базовая оценка 7.4 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
CWE-297

Уязвимость Риск: Средний

ALTXID-324281

Описание

Подписывание SMB2 пакетов включено, но не обязательно

Ссылки

ALTXID-324281

CVSSv2: Базовая оценка 6.1 (AV:A/AC:H/Au:N/C:C/I:C/A:N)
CVSSv3: Базовая оценка 3.7 (AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N)
CWE-311

MS

https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2

Уязвимость Риск: Средний

CVE-2022-28330

Описание

Apache HTTP Server 2.4.53 и более ранних версий в Windows может читать за пределами выделенной памяти, если он настроен на обработку запросов с помощью модуля mod_isapi.

Ссылки

CVE-2022-28330

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28330

CONFIRM

https://security.netapp.com/advisory/ntap-20220624-0005/

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MLIST

http://www.openwall.com/lists/oss-security/2022/06/08/3

Уязвимость Риск: Средний

CVE-2022-30556

Описание

Apache HTTP Server 2.4.53 и более ранние версии могут возвращать приложениям, вызывающим r:wsread(), длины,

которые указывают на конец хранилища, выделенного для буфера.

Ссылки

CVE-2022-30556

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
NVD-CWE-Other
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30556
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/YPY2BLEVJWFH34AX77ZJPLD2OOBYR6ND/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7QUGG2QZWHTITMABFLVXA4DNYUOTPWYQ/

CONFIRM

https://security.netapp.com/advisory/ntap-20220624-0005/

GENTOO

https://security.gentoo.org/glsa/202208-20

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MLIST

http://www.openwall.com/lists/oss-security/2022/06/08/7

Уязвимость Риск: Средний

CVE-2022-29404

Описание

В Apache HTTP Server 2.4.53 и более ранних версиях вредоносный запрос к скрипту lua, вызывающему r:parsebody(0), может вызвать отказ в обслуживании из-за отсутствия ограничения по умолчанию на возможный размер входных данных.

Ссылки

CVE-2022-29404

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-770
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29404
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/YPY2BLEVJWFH34AX77ZJPLD2OOBYR6ND/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7QUGG2QZWHTITMABFLVXA4DNYUOTPWYQ/

CONFIRM

https://security.netapp.com/advisory/ntap-20220624-0005/

GENTOO

https://security.gentoo.org/glsa/202208-20

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MLIST

http://www.openwall.com/lists/oss-security/2022/06/08/5

Уязвимость Риск: Средний

CVE-2021-44224

Описание

Уязвимость в Apache HTTP Server версии с 2.4.7 до 2.4.51 при включенном ProxyRequests может вызвать падение (разыменование нулевого указателя) привести к межсерверной подделке запросов (SSRF).

Ссылки

CVE-2021-44224

CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:N/I:P/A:P)
CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)
CWE-476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44224
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/BFSWOH4X77CV7AH7C4RMHUBDWKQDL4YH/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RGWILBORT67SHMSLYSQZG2NMXGCMPUZO/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Z7H26WJ6TPKNWV3QKY4BHKUKQVUTZJTD/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/X73C35MMMZGBVPQQCH7LQZUMYZNQA5FO/

CONFIRM
https://security.netapp.com/advisory/ntap-20211224-0001/

CONFIRM
https://www.tenable.com/security/tns-2022-01

CONFIRM
https://www.tenable.com/security/tns-2022-03

CONFIRM
https://support.apple.com/kb/HT213255

CONFIRM
https://support.apple.com/kb/HT213256

CONFIRM
https://support.apple.com/kb/HT213257

DEBIAN
https://www.debian.org/security/2022/dsa-5035

FULLDISC
http://seclists.org/fulldisclosure/2022/May/38

FULLDISC
http://seclists.org/fulldisclosure/2022/May/33

FULLDISC
http://seclists.org/fulldisclosure/2022/May/35

GENTOO
https://security.gentoo.org/glsa/202208-20

MISC
http://httpd.apache.org/security/vulnerabilities_24.html

MISC
https://www.oracle.com/security-alerts/cpujan2022.html

MISC
https://www.oracle.com/security-alerts/cpuapr2022.html

MLIST
http://www.openwall.com/lists/oss-security/2021/12/20/3

Уязвимость Риск: Средний

CVE-2022-28615

Описание

Apache HTTP Server 2.4.53 и более ранние версии могут аварийно завершить работу или раскрыть информацию из-за чтения за пределами выделенной памяти в ap_strcmp_match(), когда предоставляется очень большой входной буфер. Хотя код, распространяемый вместе с сервером, не может быть принужден к такому вызову, сторонние модули или lua-скрипты, использующие ap_strcmp_match(), гипотетически могут быть затронуты.

Ссылки

CVE-2022-28615
CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)
CWE-190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28615
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/YPY2BLEVJWFH34AX77ZJPLD2OOBYR6ND/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7QUGG2QZWHTITMABFLVXA4DNYUOTPWYQ/

CONFIRM
https://security.netapp.com/advisory/ntap-20220624-0005/

GENTOO
https://security.gentoo.org/glsa/202208-20

MISC
https://httpd.apache.org/security/vulnerabilities_24.html

MLIST
http://www.openwall.com/lists/oss-security/2022/06/08/9

Уязвимость Риск: Средний

CVE-2022-22719

Описание

Уязвимость в Apache HTTP Server до 2.4.52 может привести к сбою процесса из-за специально сформированного тела запроса.

Ссылки

CVE-2022-22719
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-665
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22719
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RGWILBORT67SHMSLYSQZG2NMXGCMPUZO/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Z7H26WJ6TPKNWV3QKY4BHKUKQVUTZJTD/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/X73C35MMMZGBVPQQCH7LQZUMYZNQA5FO/

CONFIRM
https://security.netapp.com/advisory/ntap-20220321-0001/

CONFIRM
https://support.apple.com/kb/HT213256

CONFIRM
https://support.apple.com/kb/HT213257

CONFIRM
https://support.apple.com/kb/HT213255

FULLDISC
http://seclists.org/fulldisclosure/2022/May/38

FULLDISC
http://seclists.org/fulldisclosure/2022/May/33

FULLDISC
http://seclists.org/fulldisclosure/2022/May/35

GENTOO
https://security.gentoo.org/glsa/202208-20

MISC
https://httpd.apache.org/security/vulnerabilities_24.html

MISC
https://www.oracle.com/security-alerts/cpuapr2022.html

MLIST
http://www.openwall.com/lists/oss-security/2022/03/14/4

MLIST
https://lists.debian.org/debian-lts-announce/2022/03/msg00033.html

Уязвимость Риск: Средний

CVE-2022-26377

Описание

Уязвимость «Несогласованная интерпретация HTTP-запросов» («Контрабанда HTTP-запросов») в mod_proxy_ajp сервера Apache HTTP Server позволяет злоумышленнику незаконно передавать запросы на сервер AJP, на который он перенаправляет запросы. Эта проблема затрагивает Apache HTTP Server Apache HTTP Server 2.4 версии 2.4.53 и предыдущие версии.

Ссылки

CVE-2022-26377
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CWE-444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26377
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/YPY2BLEVJWFH34AX77ZJPLD2OOBYR6ND/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7QUGG2QZWHTITMABFLVXA4DNYUOTPWYQ/

CONFIRM
https://security.netapp.com/advisory/ntap-20220624-0005/

GENTOO
https://security.gentoo.org/glsa/202208-20

MISC
https://httpd.apache.org/security/vulnerabilities_24.html

MLIST
http://www.openwall.com/lists/oss-security/2022/06/08/2

Уязвимость Риск: Средний

CVE-2022-28614

Описание

Функция ap_rwrite() в Apache HTTP Server 2.4.53 и более ранних версиях может считывать память, если злоумышленник может заставить сервер отражать очень большие входные данные с помощью ap_rwrite() или ap_rputs(), например, с помощью функции mod_luas r:puts(). Для решения проблемы модули, скомпилированные и распространяемые отдельно от Apache HTTP Server, которые используют функцию 'ap_rputs' и могут передавать ей очень большие (INT_MAX или больше) строки, должны быть скомпилированы с текущими заголовками.

Ссылки

CVE-2022-28614
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28614
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/YPY2BLEVJWFH34AX77ZJPLD2OOBYR6ND/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7QUGG2QZWHTITMABFLVXA4DNYUOTPWYQ/

CONFIRM
https://security.netapp.com/advisory/ntap-20220624-0005/

GENTOO

https://security.gentoo.org/glsa/202208-20

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MLIST

http://www.openwall.com/lists/oss-security/2022/06/08/4

Уязвимость Риск: Средний

CVE-2022-22721

Описание

Целочисленное переполнение в Apache HTTP Server до 2.4.52.

Ссылки

CVE-2022-22721

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:N/I:P/A:P)
CVSSv3: Базовая оценка 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)
CWE-190

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22721

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RGWILBORT67SHMSLYSQZG2NMXGCMPUZO/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Z7H26WJ6TPKNWV3QKY4BHKUKQVUTZJTD/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/X73C35MMMZGBVPQQCH7LQZUMYZNQA5FO/

CONFIRM

https://security.netapp.com/advisory/ntap-20220321-0001/

CONFIRM

https://support.apple.com/kb/HT213256

CONFIRM

https://support.apple.com/kb/HT213257

CONFIRM

https://support.apple.com/kb/HT213255

FULLDISC

http://seclists.org/fulldisclosure/2022/May/38

FULLDISC

http://seclists.org/fulldisclosure/2022/May/33

FULLDISC

http://seclists.org/fulldisclosure/2022/May/35

GENTOO

https://security.gentoo.org/glsa/202208-20

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MISC

https://www.oracle.com/security-alerts/cpuapr2022.html

MLIST

http://www.openwall.com/lists/oss-security/2022/03/14/2

MLIST

https://lists.debian.org/debian-lts-announce/2022/03/msg00033.html

N/A

https://www.oracle.com/security-alerts/cpujul2022.html

Уязвимость Риск: Средний

ALTXID-340429

Описание

Обнаружены резервные копии файлов на веб сервере. Не рекомендуется хранить бэкапы на том же диске, что и исходные данные.

Ссылки

ALTXID-340429

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.8 (AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N)

Уязвимость Риск: Средний

ALTXID-338287

Описание

Обнаружен потенциально опасный http метод TRACE. Этот метод возвращает в ответе клиенту строку, которая была ему послана и используется в большинстве случаев для отладки. Но также этот метод может быть использован для проведения атаки Cross Site Tracing (XST). Рекомендуется отключить метод.

Ссылки

ALTXID-338287

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-16

Уязвимость Риск: Средний

CVE-2017-9118

Описание

Доступ за пределами выделенной памяти в php_pcre_replace_impl в PHP 7.1.5 через специально сформированный preg_replace вызов.

Ссылки

CVE-2017-9118

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9118

CONFIRM

https://security.netapp.com/advisory/ntap-20181107-0003/

MISC

https://bugs.php.net/bug.php?id=74604

REDHAT

https://access.redhat.com/errata/RHSA-2019:2519

Уязвимость Риск: Средний

CVE-2020-7071

Описание

В версиях PHP 7.3.x ниже 7.3.26, 7.4.x ниже 7.4.14 и 8.0.0 при проверке URL-адреса с помощью таких функций, как filter_var ($ url, FILTER_VALIDATE_URL), PHP примет URL-адрес с недействительным паролем, как действительный URL. Это может привести к тому, что функции, которые полагаются на действительность URL-адреса, неправильно проанализируют URL-адрес и выдадут неверные данные в качестве компонентов URL-адреса.

Ссылки

CVE-2020-7071

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CWE-20
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7071

CONFIRM
https://bugs.php.net/bug.php?id=77423

CONFIRM
https://security.netapp.com/advisory/ntap-20210312-0005/

CONFIRM
https://www.tenable.com/security/tns-2021-14

DEBIAN
https://www.debian.org/security/2021/dsa-4856

GENTOO
https://security.gentoo.org/glsa/202105-23

MISC
https://www.oracle.com/security-alerts/cpuoct2021.html

MLIST
https://lists.debian.org/debian-lts-announce/2021/07/msg00008.html

Уязвимость Риск: Средний

CVE-2021-21702

Описание

В версиях PHP 7.3.x ниже 7.3.27, 7.4.x ниже 7.4.15 и 8.0.x ниже 8.0.2 при использовании расширения SOAP для подключения к серверу SOAP злонамеренный сервер SOAP в качестве ответа может возвращать XML-данные неверного формата, что заставит PHP обратиться к нулевому указателю и, таким образом, вызвать сбой.

Ссылки

CVE-2021-21702
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21702

CONFIRM
https://bugs.php.net/bug.php?id=80672

CONFIRM
https://security.netapp.com/advisory/ntap-20210312-0005/

CONFIRM
https://www.tenable.com/security/tns-2021-14

DEBIAN
https://www.debian.org/security/2021/dsa-4856

GENTOO
https://security.gentoo.org/glsa/202105-23

MISC
https://www.oracle.com/security-alerts/cpuoct2021.html

MLIST
https://lists.debian.org/debian-lts-announce/2021/07/msg00008.html

Уязвимость Риск: Средний

CVE-2021-21706

Описание

Уязвимость в PHP версии 7.3.x до 7.3.31, 7.4.x до 7.4.24 и 8.0.x до 8.0.11, в ZipArchive::extractTo может привести к созданию или перезаписи файлов в зависимости от разрешений операционной системы.

Ссылки

CVE-2021-21706

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)
CWE-22
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21706

CONFIRM
https://bugs.php.net/bug.php?id=81420

CONFIRM
https://security.netapp.com/advisory/ntap-20211029-0007/

Уязвимость Риск: Средний

CVE-2021-21705

Описание

Уязвимость в PHP версии 7.3.x до 7.3.29, 7.4.x до 7.4.21 и 8.0.x до 8.0.8 при проверке URL.

Ссылки

CVE-2021-21705
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CWE-20
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21705

CONFIRM
https://bugs.php.net/bug.php?id=81122

CONFIRM
https://security.netapp.com/advisory/ntap-20211029-0006/

GENTOO
https://security.gentoo.org/glsa/202209-20

MISC
https://www.oracle.com/security-alerts/cpujan2022.html

Уязвимость Риск: Средний

CVE-2021-21704

Описание

Уязвимость в PHP версии 7.3.x до 7.3.29, 7.4.x до 7.4.21 и 8.0.x до 8.0.8 при использовании Firebird PDO драйвера может привести к отказу в обслуживании или повреждению памяти.

Ссылки

CVE-2021-21704
CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21704

CONFIRM
https://bugs.php.net/bug.php?id=76450

CONFIRM
https://bugs.php.net/bug.php?id=76452

CONFIRM
https://bugs.php.net/bug.php?id=76449

CONFIRM
https://bugs.php.net/bug.php?id=76448

CONFIRM
https://security.netapp.com/advisory/ntap-20211029-0006/

GENTOO
https://security.gentoo.org/glsa/202209-20

Уязвимость Риск: Средний

CVE-2021-21708

Описание

В версиях PHP 7.4.x ниже 7.4.28, 8.0.x ниже 8.0.16 и 8.1.x ниже 8.1.3 при использовании функций фильтра с фильтром FILTER_VALIDATE_FLOAT и min/max ограничением, если фильтр не работает, существует возможность инициировать использование выделенной памяти после освобождения, что может привести к ее сбою и, возможно, к перезаписи других фрагментов памяти и RCE. Эта проблема затрагивает: код, который использует FILTER_VALIDATE_FLOAT с минимальными/максимальными ограничениями.

Ссылки

CVE-2021-21708
CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-416
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21708

CONFIRM
https://bugs.php.net/bug.php?id=81708

CONFIRM
https://security.netapp.com/advisory/ntap-20220325-0004/

GENTOO
https://security.gentoo.org/glsa/202209-20

Уязвимость Риск: Средний

CVE-2021-21707

Описание

В PHP версии 7.3.x до 7.3.33, 7.4.x до 7.4.26 и 8.0.x до 8.0.13 некоторые функции анализа XML, такие как simplexml_load_file(), некорректно декодируют переданное имя файла, что может привести к чтению другого файла.

Ссылки

CVE-2021-21707
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
NVD-CWE-Other
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21707

CONFIRM
https://security.netapp.com/advisory/ntap-20211223-0005/

CONFIRM
https://www.tenable.com/security/tns-2022-09

DEBIAN
https://www.debian.org/security/2022/dsa-5082

MISC
https://bugs.php.net/bug.php?id=79971

MLIST
https://lists.debian.org/debian-lts-announce/2022/12/msg00030.html

Уязвимость Риск: Средний

CVE-2022-31625

Описание

Использование неинициализированной памяти в pg_query_params() в PHP до 8.0.20 и до 8.1.7 и до 7.4.30.

Ссылки

CVE-2022-31625

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31625
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZZTZQKRGEYJT5UB4FGG3MOE72SQUHSL4/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3T4MMEEZYYAEHPQMZDFN44PHORJWJFZQ/

CONFIRM

https://security.netapp.com/advisory/ntap-20220722-0005/

DEBIAN

https://www.debian.org/security/2022/dsa-5179

GENTOO

https://security.gentoo.org/glsa/202209-20

MISC

https://bugs.php.net/bug.php?id=81720

MLIST

https://lists.debian.org/debian-lts-announce/2022/12/msg00030.html

Уязвимость Риск: Средний

CVE-2021-21703

Описание

Уязвимость повреждения памяти в PHP до 8.0.12 и до 7.3.32 и до 7.4.25 позволяет повысить привилегии.

Ссылки

CVE-2021-21703

CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)
CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21703
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/JO5RA6YOBGGGKLIA6F6BQRZDDECF5L3R/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/PBM3KKB3RY2YPOKNMC4HIH7IH3T3WC74/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6PZVLICZUJMXOGWOUWSBAEGIVTF6Y6V3/

CONFIRM

https://security.netapp.com/advisory/ntap-20211118-0003/

DEBIAN

https://www.debian.org/security/2021/dsa-4993

DEBIAN

https://www.debian.org/security/2021/dsa-4992

GENTOO

https://security.gentoo.org/glsa/202209-20

MISC

https://bugs.php.net/bug.php?id=81026

MISC

https://www.oracle.com/security-alerts/cpujan2022.html

MISC

https://www.oracle.com/security-alerts/cpuapr2022.html

MLIST

http://www.openwall.com/lists/oss-security/2021/10/26/7

MLIST

https://lists.debian.org/debian-lts-announce/2021/10/msg00021.html

Уязвимость Риск: Средний

CVE-2020-7070

Описание

Уязвимость в обработке значений HTTP cookie в PHP версии 7.2.x до 7.2.34, 7.3.x до 7.3.23 и 7.4.x до 7.4.11 позволяет злоумышленнику подделать cookie.

Ссылки

CVE-2020-7070

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CWE-565
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7070
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RRU57N3OSYZPOMFWPRDNVH7EMYOTSZ66/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7EVDN7D3IB4EAI4D3ZOM2OJKQ5SD7K4E/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/P2J3ZZDHCSX65T5QWV4AHBN7MOJXBEKG/

CONFIRM

https://security.netapp.com/advisory/ntap-20201016-0001/

CONFIRM

https://www.tenable.com/security/tns-2021-14

DEBIAN

https://www.debian.org/security/2021/dsa-4856

GENTOO

https://security.gentoo.org/glsa/202012-16

MISC

https://bugs.php.net/bug.php?id=79699

MISC

http://cve.circl.lu/cve/CVE-2020-8184

MISC

https://hackerone.com/reports/895727

MISC

https://www.oracle.com/security-alerts/cpuoct2021.html

MLIST

https://lists.debian.org/debian-lts-announce/2020/10/msg00008.html

SUSE

http://lists.opensuse.org/opensuse-security-announce/2020-10/msg00045.html

SUSE

http://lists.opensuse.org/opensuse-security-announce/2020-10/msg00067.html

UBUNTU

https://usn.ubuntu.com/4583-1/

Уязвимость Риск: Средний

CVE-2022-31626

Описание

Переполнение буфера в PHP до 8.0.20 и до 8.1.7 и до 7.4.30.

Ссылки

CVE-2022-31626

CVSSv2: Базовая оценка 6.0 (AV:N/AC:M/Au:S/C:P/I:P/A:P)
CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-120
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31626
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZZTZQKRGEYJT5UB4FGG3MOE72SQUHSL4/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3T4MMEEZYYAEHPQMZDFN44PHORJWJFZQ/

CONFIRM
https://security.netapp.com/advisory/ntap-20220722-0005/

DEBIAN
https://www.debian.org/security/2022/dsa-5179

GENTOO
https://security.gentoo.org/glsa/202209-20

MISC
https://bugs.php.net/bug.php?id=81719

MLIST
https://lists.debian.org/debian-lts-announce/2022/12/msg00030.html

Уязвимость Риск: Средний

CVE-2020-7069

Описание

Уязвимость в PHP версии 7.2.x до 7.2.34, 7.3.x до 7.3.23 и 7.4.x до 7.4.11, когда AES-CCM mode используется, может привести как к снижению безопасности, так и к некорректному шифрованию данных.

Ссылки

CVE-2020-7069
CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
CWE-326
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7069
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RRU57N3OSYZPOMFWPRDNVH7EMYOTSZ66/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7EVDN7D3IB4EAI4D3ZOM2OJKQ5SD7K4E/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/P2J3ZZDHCSX65T5QWV4AHBN7MOJXBEKG/

CONFIRM
https://security.netapp.com/advisory/ntap-20201016-0001/

CONFIRM
https://www.tenable.com/security/tns-2021-14

DEBIAN
https://www.debian.org/security/2021/dsa-4856

GENTOO
https://security.gentoo.org/glsa/202012-16

MISC
https://bugs.php.net/bug.php?id=79601

MISC
https://www.oracle.com/security-alerts/cpuApr2021.html

MISC
https://www.oracle.com/security-alerts/cpuoct2021.html

SUSE
http://lists.opensuse.org/opensuse-security-announce/2020-10/msg00045.html

SUSE

http://lists.opensuse.org/opensuse-security-announce/2020-10/msg00067.html

UBUNTU

https://usn.ubuntu.com/4583-1/

Уязвимость Риск: Средний

CVE-2019-1551

Описание

Ошибка переполнения в OpenSSL 1.1.1-1.1.1d и 1.0.2-1.0.2t.

Ссылки

CVE-2019-1551

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1551
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/XVEP3LAK4JSPRXFO4QF4GG2IVXADV3SO/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/DDHOAATPWJCXRNFMJ2SASDBBNU5RJONY/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/EXDDAOWSAIEFQNBHWYE6PPYFV4QXGMCD/
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=419102400a2811582a7a3d4a4e317d72e5ce0a8f
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=f1c5eea8a817075d31e43f5876993c6710238c98

BUGTRAQ

https://seclists.org/bugtraq/2019/Dec/39

BUGTRAQ

https://seclists.org/bugtraq/2019/Dec/46

CONFIRM

https://www.openssl.org/news/secadv/20191206.txt

CONFIRM

https://security.netapp.com/advisory/ntap-20191210-0001/

CONFIRM

https://www.tenable.com/security/tns-2019-09

CONFIRM

https://www.tenable.com/security/tns-2020-03

CONFIRM

https://www.tenable.com/security/tns-2020-11

CONFIRM

https://www.tenable.com/security/tns-2021-10

DEBIAN

https://www.debian.org/security/2019/dsa-4594

DEBIAN

https://www.debian.org/security/2021/dsa-4855

GENTOO

https://security.gentoo.org/glsa/202004-10

MISC

http://packetstormsecurity.com/files/155754/Slackware-Security-Advisory-openssl-Updates.html

MISC

https://www.oracle.com/security-alerts/cpujul2020.html

MISC

https://www.oracle.com/security-alerts/cpujan2021.html

MISC

https://www.oracle.com/security-alerts/cpuApr2021.html

MLIST
https://lists.debian.org/debian-lts-announce/2022/03/msg00023.html
SUSE
http://lists.opensuse.org/opensuse-security-announce/2020-01/msg00030.html
UBUNTU
https://usn.ubuntu.com/4376-1/
UBUNTU
https://usn.ubuntu.com/4504-1/

Уязвимость Риск: Средний

CVE-2018-0735

Описание

Уязвимость в алгоритме подписи OpenSSL ECDSA, злоумышленник может использовать различные варианты алгоритма подписи для восстановления закрытого ключа. Испралено в OpenSSL 1.1.0j-dev (1.1.0-1.1.0i). Испралено в OpenSSL 1.1.1a-dev (1.1.1).

Ссылки

CVE-2018-0735
CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.0 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
CWE-327
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0735
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=56fb454d281a023b3f950d969693553d3f3ceea1
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=b1d6d55ece1c26fa2829e2b819b038d7b6d692b4
BID
http://www.securityfocus.com/bid/105750
CONFIRM
https://www.openssl.org/news/secadv/20181029.txt
CONFIRM
https://security.netapp.com/advisory/ntap-20181105-0002/
CONFIRM
https://nodejs.org/en/blog/vulnerability/november-2018-security-releases/
CONFIRM
https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
DEBIAN
https://www.debian.org/security/2018/dsa-4348
MISC
https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
MISC
https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
MISC
https://www.oracle.com/security-alerts/cpujan2020.html
MLIST
https://lists.debian.org/debian-lts-announce/2018/11/msg00024.html
REDHAT
https://access.redhat.com/errata/RHSA-2019:3700
SECTRACK
http://www.securitytracker.com/id/1041986
UBUNTU
https://usn.ubuntu.com/3840-1/

Уязвимость Риск: Средний

CVE-2021-23840

Описание

Уязвимость в EVP_CipherUpdate, EVP_EncryptUpdate и EVP_DecryptUpdate в OpenSSL 1.1.1 до 1.1.1i, и 1.0.2 до 1.0.2x может привести к отказу в обслуживании.

Ссылки

CVE-2021-23840

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23840
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=6a51b9e1d0cf0bf8515f7201b68fb0a3482b3dc1
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=9b1129239f3ebb1d1c98ce9ed41d5c9476c47cb2
https://lists.apache.org/thread.html/rf4c02775860db415b4955778a131c2795223f61cb8c6a450893651e4%40%3Cissues.bookkeeper.apache.org%3E
https://lists.apache.org/thread.html/r58af02e294bd07f487e2c64ffc0a29b837db5600e33b6e698b9d696b%40%3Cissues.bookkeeper.apache.org%3E

CONFIRM
https://www.openssl.org/news/secadv/20210216.txt

CONFIRM
https://security.netapp.com/advisory/ntap-20210219-0009/

CONFIRM
https://www.tenable.com/security/tns-2021-03

CONFIRM
https://www.tenable.com/security/tns-2021-09

CONFIRM
https://www.tenable.com/security/tns-2021-10

CONFIRM
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44846

CONFIRM
https://kc.mcafee.com/corporate/index?page=content&id=SB10366

CONFIRM
https://cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf

DEBIAN
https://www.debian.org/security/2021/dsa-4855

GENTOO
https://security.gentoo.org/glsa/202103-03

MISC
https://www.oracle.com/security-alerts/cpuApr2021.html

MISC
https://www.oracle.com/security-alerts/cpuoct2021.html

MISC
https://www.oracle.com/security-alerts/cpujan2022.html

MISC
https://www.oracle.com/security-alerts/cpuapr2022.html

N/A
https://www.oracle.com//security-alerts/cpujul2021.html

Уязвимость Риск: Средний

CVE-2021-3712

Описание

Уязвимость в OpenSSL 1.1.1 до 1.1.1k, и 1.0.2 до 1.0.2y может вызвать атаку "Отказ в обслуживании", а также привести к раскрытию содержимого памяти.

Ссылки

CVE-2021-3712

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:N/A:P)
CVSSv3: Базовая оценка 7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H)
CWE-125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3712
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=94d23fcff9b2a7a8368dfe52214d5c2569882c11
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=ccb0a11145ee72b042d10593a64eaf9e8a55ec12
https://lists.apache.org/thread.html/r18995de860f0e63635f3008fd2a6aca82394249476d21691e7c59c9e%40%3Cdev.tomcat.apache.org%3E
https://lists.apache.org/thread.html/rad5d9f83f0d11fb3f8bb148d179b8a9ad7c6a17f18d70e5805a713d1%40%3Cdev.tomcat.apache.org%3E

CONFIRM
https://www.openssl.org/news/secadv/20210824.txt

CONFIRM
https://security.netapp.com/advisory/ntap-20210827-0010/

CONFIRM
https://www.tenable.com/security/tns-2021-16

CONFIRM
https://kc.mcafee.com/corporate/index?page=content&id=SB10366

CONFIRM
https://www.tenable.com/security/tns-2022-02

CONFIRM
https://cert-portal.siemens.com/productcert/pdf/ssa-244969.pdf

CONFIRM
https://cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf

DEBIAN
https://www.debian.org/security/2021/dsa-4963

GENTOO
https://security.gentoo.org/glsa/202209-02

GENTOO
https://security.gentoo.org/glsa/202210-02

MISC
https://www.oracle.com/security-alerts/cpuoct2021.html

MISC
https://www.oracle.com/security-alerts/cpujan2022.html

MISC
https://www.oracle.com/security-alerts/cpuapr2022.html

MLIST
http://www.openwall.com/lists/oss-security/2021/08/26/2

MLIST
https://lists.debian.org/debian-lts-announce/2021/09/msg00014.html

MLIST
https://lists.debian.org/debian-lts-announce/2021/09/msg00021.html

Уязвимость Риск: Средний

CVE-2019-1563

Описание

Уязвимость в OpenSSL до 1.1.1d, до 1.1.0l и до 1.0.2t позволяет восстановить CMS/PKCS7 транспортированный ключ шифрования или расшифровать любое сообщение, которое было зашифровано с помощью открытого ключа RSA.

Ссылки

CVE-2019-1563

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-327
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1563
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/GY6SNRJP2S7Y42GIIDO3HXPNMDYN2U3A/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZN4VVQJ3JDCHGIHV4Y2YTXBYQZ6PWQ7E/
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=08229ad838c50f644d7e928e2eef147b4308ad64
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=631f94db0065c78181ca9ba5546ebc8bb3884b97
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=e21f8cf78a125cd3c8c0d1a1a6c8bb0b901f893f
https://support.f5.com/csp/article/K97324400?utm_source=f5support&amp%3Butm_medium=RSS

BUGTRAQ
https://seclists.org/bugtraq/2019/Sep/25

BUGTRAQ
https://seclists.org/bugtraq/2019/Oct/0

BUGTRAQ
https://seclists.org/bugtraq/2019/Oct/1

CONFIRM
https://www.openssl.org/news/secadv/20190910.txt

CONFIRM
https://security.netapp.com/advisory/ntap-20190919-0002/

CONFIRM
https://kc.mcafee.com/corporate/index?page=content&id=SB10365

CONFIRM
https://www.tenable.com/security/tns-2019-09

DEBIAN
https://www.debian.org/security/2019/dsa-4540

DEBIAN
https://www.debian.org/security/2019/dsa-4539

GENTOO
https://security.gentoo.org/glsa/201911-04

MISC
http://packetstormsecurity.com/files/154467/Slackware-Security-Advisory-openssl-Updates.html

MISC
https://www.oracle.com/security-alerts/cpuoct2020.html

MISC
https://www.oracle.com/security-alerts/cpujul2020.html

MISC
https://www.oracle.com/security-alerts/cpujan2020.html

MISC
https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

MLIST
https://lists.debian.org/debian-lts-announce/2019/09/msg00026.html

N/A
https://www.oracle.com/security-alerts/cpuapr2020.html

SUSE
http://lists.opensuse.org/opensuse-security-announce/2019-09/msg00054.html

SUSE
http://lists.opensuse.org/opensuse-security-announce/2019-09/msg00072.html

SUSE
http://lists.opensuse.org/opensuse-security-announce/2019-10/msg00016.html

SUSE
http://lists.opensuse.org/opensuse-security-announce/2019-10/msg00012.html

UBUNTU

https://usn.ubuntu.com/4504-1/

UBUNTU

https://usn.ubuntu.com/4376-2/

UBUNTU

https://usn.ubuntu.com/4376-1/

Уязвимость Риск: Средний

CVE-2021-4160

Описание

OpenSSL 1.0.2, 1.1.1 и 3.0.0. В процедуре возведения в квадрат MIPS32 и MIPS64 обнаружена ошибка распространения переноса. Затронуты многие алгоритмы EC, включая некоторые кривые по умолчанию TLS 1.3. Атаки на RSA и DSA-серверы считаются маловероятными. Атаки на DH считаются осуществимыми, но сложными. Исправлено в 1.1.1m, 1.0.2zc-dev, 3.0.1.

Ссылки

CVE-2021-4160

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
NVD-CWE-noinfo
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4160
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=3bf7b73ea7123045b8f972badc67ed6878e6c37f
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=e9e726506cd2a3fd9c0f12daf8cc1fe934c7dddb
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=6fc1aaaf303185aa5e483e06bdfae16daa9193a7

CONFIRM

https://www.openssl.org/news/secadv/20220128.txt

CONFIRM

https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

DEBIAN

https://www.debian.org/security/2022/dsa-5103

GENTOO

https://security.gentoo.org/glsa/202210-02

MISC

https://www.oracle.com/security-alerts/cpuapr2022.html

N/A

https://www.oracle.com/security-alerts/cpujul2022.html

Уязвимость Риск: Средний

CVE-2019-0190

Описание

Уязвимость в Apache HTTP Server версии 2.4.37.

Ссылки

CVE-2019-0190

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
NVD-CWE-noinfo
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0190
https://lists.apache.org/thread.html/56c2e7cc9deb1c12a843d0dc251ea7fd3e7e80293cde02fcd65286ba%40%3Ccvs.httpd.apache.org%3E
https://lists.apache.org/thread.html/84a3714f0878781f6ed84473d1a503d2cc382277e100450209231830%40%3Ccvs.httpd.apache.org%3E
https://lists.apache.org/thread.html/rd18c3c43602e66f9cdcf09f1de233804975b9572b0456cc582390b6f%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/re3d27b6250aa8548b8845d314bb8a350b3df326cacbbfdfe4d455234%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/rf6449464fd8b7437704c55f88361b66f12d5b5f90bcce66af4be4ba9%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/r06f0d87ebb6d59ed8379633f36f72f5b1f79cadfda72ede0830b42cf%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/rc998b18880df98bafaade071346690c2bc1444adaa1a1ea464b93f0a%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/r03ee478b3dda3e381fd6189366fa7af97c980d2f602846eef935277d%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/rd2fb621142e7fa187cfe12d7137bf66e7234abcbbcd800074c84a538%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/r9f93cf6dde308d42a9c807784e8102600d0397f5f834890708bf6920%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/re473305a65b4db888e3556e4dae10c2a04ee89dcff2e26ecdbd860a9%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/rd336919f655b7ff309385e34a143e41c503e133da80414485b3abcc9%40%3Ccvs.httpd.apache.org%3E

https://lists.apache.org/thread.html/r76142b8c5119df2178be7c2dba88fde552eedeec37ea993dfce68d1d%40%3Ccvs.httpd.apache.org%3E

BID

http://www.securityfocus.com/bid/106743

CONFIRM

https://httpd.apache.org/security/vulnerabilities_24.html

CONFIRM

https://security.netapp.com/advisory/ntap-20190125-0001/

GENTOO

https://security.gentoo.org/glsa/201903-21

MISC

https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

MISC

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

N/A

https://www.oracle.com//security-alerts/cpujul2021.html

Уязвимость Риск: Средний

CVE-2019-1549

Описание

OpenSSL до 1.1.1d не использовал по умолчанию генератор случайных чисел (RNG) для защиты в случае системного вызова fork().

Ссылки

CVE-2019-1549

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 4.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)
CWE-330
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1549

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/GY6SNRJP2S7Y42GIIDO3HXPNMDYN2U3A/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZN4VVQJ3JDCHGIHV4Y2YTXBYQZ6PWQ7E/

https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=1b0fe00e2704b5e20334a16d3c9099d1ba2ef1be

https://support.f5.com/csp/article/K44070243?utm_source=f5support&amp%3Butm_medium=RSS

BUGTRAQ

https://seclists.org/bugtraq/2019/Oct/1

CONFIRM

https://www.openssl.org/news/secadv/20190910.txt

CONFIRM

https://security.netapp.com/advisory/ntap-20190919-0002/

CONFIRM

https://support.f5.com/csp/article/K44070243

DEBIAN

https://www.debian.org/security/2019/dsa-4539

MISC

https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

MISC

https://www.oracle.com/security-alerts/cpujan2020.html

MISC

https://www.oracle.com/security-alerts/cpujul2020.html

MISC

https://www.oracle.com/security-alerts/cpuoct2020.html

N/A

https://www.oracle.com/security-alerts/cpuapr2020.html

UBUNTU

https://usn.ubuntu.com/4376-1/

Уязвимость Риск: Средний

CVE-2019-1543

Описание

Раскрытие информации в OpenSSL в шифре ChaCha20-Poly1305. Уязвимы версии 1.1.1 до 1.1.1b, и 1.1.0 до 1.1.0j.

Ссылки

CVE-2019-1543

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSSv3: Базовая оценка 2.9 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
CWE-327

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1543

https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=f426625b6ae9a7831010750490a5f0ad689c5ba3

https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=ee22257b1418438ebaf54df98af4e24f494d1809

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZBEV5QGDRFUZDMNECFXUSN5FMYOZDE4V/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Y3IVFGSERAZLNJCK35TEM2R4726XIH3Z/

BUGTRAQ

https://seclists.org/bugtraq/2019/Jul/3

CONFIRM

https://www.openssl.org/news/secadv/20190306.txt

CONFIRM

https://kc.mcafee.com/corporate/index?page=content&id=SB10365

DEBIAN

https://www.debian.org/security/2019/dsa-4475

MISC

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

MISC

https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

N/A

https://www.oracle.com/security-alerts/cpuapr2020.html

REDHAT

https://access.redhat.com/errata/RHSA-2019:3700

SUSE

http://lists.opensuse.org/opensuse-security-announce/2019-07/msg00056.html

Уязвимость Риск: Средний

CVE-2020-15400

Описание

CakePHP до 4.0.6 неправильно обрабатывает генерацию токенов CSRF. Это может быть удаленно использовано вместе с XSS.

Ссылки

CVE-2020-15400

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CVSSv3: Базовая оценка 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)
CWE-352
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15400

MISC

https://bakery.cakephp.org/2020/04/18/cakephp_406_released.html

Уязвимость Риск: Средний

CVE-2006-5031

Описание

Уязвимость обхода каталогов в app/webroot/js/vendors.php в Cake Software Foundation CakePHP до 1.1.8.3544 позволяет считывать произвольные файлы через .. (dot dot) в параметре файла, за которым следует имя файла, заканчивающееся на "%00", и имя файла .js.

Ссылки

CVE-2006-5031

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE-22
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5031

BID

http://www.securityfocus.com/bid/20150

CONFIRM

http://cakeforge.org/frs/shownotes.php?release_id=134

MISC

http://www.gulftech.org/?node=research&article_id=00114-09212006

SECUNIA

http://secunia.com/advisories/22040

XF

https://exchange.xforce.ibmcloud.com/vulnerabilities/29115

Уязвимость Риск: Средний

CVE-2006-4067

Описание

Уязвимость межсайтового скриптинга в cake/libs/error.php в CakePHP до 1.1.7.3363 позволяет внедрять произвольный веб-скрипт или HTML-код через URL, что отражается на странице с ошибкой 404 ("Не найдено").

Ссылки

CVE-2006-4067

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CWE-79
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4067

BID
http://www.securityfocus.com/bid/19372

CONFIRM
http://cakeforge.org/frs/shownotes.php?release_id=124

SECUNIA
http://secunia.com/advisories/21383

VUPEN
http://www.vupen.com/english/advisories/2006/3172

XF
https://exchange.xforce.ibmcloud.com/vulnerabilities/28256

Уязвимость Риск: Средний

ALTXID-324287

Описание

Некорректная цепочка сертификатов (самоподписанный сертификат). Не рекомендуется использовать самоподписанный сертификат.

Ссылки

ALTXID-324287
CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
CVSSv3: Базовая оценка 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
CWE-296

Уязвимость Риск: Низкий

CVE-2019-1552

Описание

OpenSSL имеет внутреннее значение по умолчанию для дерева каталогов, где он может найти файлы конфигурации и сертификаты. Этот каталог обычно называется OPENSSLDIR и настраивается с помощью параметров --prefix / --openssldir. OpenSSL версий 1.1.1-1.1.1c, 1.1.0-1.1.0k и 1.0.2-1.0.2s для mingw конфигурации предполагают, что результирующие программы и библиотеки установлены в Unix-подобной среде и префикс по умолчанию задан "/usr/local". Тем не менее, mingw-это программы Windows, и поэтому они ищут подкаталоги 'C:/usr/local', который может быть общедоступен для записи, что позволяет злоумышленникам изменять конфигурацию OpenSSL, вставлять сертификаты CA, изменять (или даже заменять) существующие модули и т.д.

Ссылки

CVE-2019-1552
CVSSv2: Базовая оценка 1.8 (AV:L/AC:M/Au:N/C:N/I:P/A:N)
CVSSv3: Базовая оценка 3.2 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)
CWE-295
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1552
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/EWC42UXL5GHTU5G77VKBF6JYUUNGSHOM/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZBEV5QGDRFUZDMNECFXUSN5FMYOZDE4V/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/Y3IVFGSERAZLNJCK35TEM2R4726XIH3Z/
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=54aa9d51b09d67e90db443f682cface795f5af9e
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=e32bc855a81a2d48d215c506bdeb4f598045f7e9
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=b15a19c148384e73338aa7c5b12652138e35ed28
https://git.openssl.org/gitweb/?p=openssl.git%3Ba=commitdiff%3Bh=d333ebaf9c77332754a9d5e111e2f53e1de54fdd
https://support.f5.com/csp/article/K94041354?utm_source=f5support&amp%3Butm_medium=RSS

CERT-VN
https://www.kb.cert.org/vuls/id/429301
CONFIRM
https://www.openssl.org/news/secadv/20190730.txt
CONFIRM
https://security.netapp.com/advisory/ntap-20190823-0006/
CONFIRM
https://cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf
CONFIRM
https://kc.mcafee.com/corporate/index?page=content&id=SB10365
CONFIRM
https://www.tenable.com/security/tns-2019-09
CONFIRM
https://www.tenable.com/security/tns-2019-08
CONFIRM
https://support.f5.com/csp/article/K94041354
MISC
https://www.oracle.com/security-alerts/cpuoct2020.html
MISC
https://www.oracle.com/security-alerts/cpujul2020.html
MISC
https://www.oracle.com/security-alerts/cpujan2020.html
MISC
https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
N/A
https://www.oracle.com/security-alerts/cpuapr2020.html

Уязвимость Риск: Низкий

ALTXID-341903

Описание

Удалось получить время запуска системы (дату последней перезагрузки). Многие обновления безопасности требуют перезагрузки системы, таким образом, можно косвенно узнать установлены ли последние патчи.

Ссылки

ALTXID-341903
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-200

Уязвимость Риск: Недоступно

CVE-2006-20001

Описание

Тщательно созданный заголовок запроса If: может привести к считыванию или записи одного нулевого байта в ячейку памяти пула (кучи) за пределами отправленного значения заголовка, что приводит к сбою процесса. Эта проблема затрагивает HTTP-сервер Apache 2.4.54 и ниже.

Ссылки

CVE-2006-20001
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-20001
MISC
https://httpd.apache.org/security/vulnerabilities_24.html

MISC
https://security.gentoo.org/glsa/202309-01

Уязвимость Риск: Недоступно

CVE-2023-25690

Описание

Некоторые конфигурации mod_proxy, если он включен вместе с какой-либо формой RewriteRule или ProxyPassMatch, на HTTP-сервере Apache 2.4.0 до 2.4.55 допускают атаку контрабанды HTTP-запросов. Рекомендуется обновить HTTP-сервер Apache до 2.4.56.

Ссылки

CVE-2023-25690
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25690
http://packetstormsecurity.com/files/176334/Apache-2.4.55-mod_proxy-HTTP-Request-Smuggling.html

MISC
https://httpd.apache.org/security/vulnerabilities_24.html

MISC
https://lists.debian.org/debian-lts-announce/2023/04/msg00028.html

MISC
https://security.gentoo.org/glsa/202309-01

Уязвимость Риск: Недоступно

CVE-2023-27522

Описание

Уязвимость для контрабанды HTTP-ответов в HTTP-сервере Apache через mod_proxy_uwsgi (HTTP-сервер Apache с 2.4.30 по 2.4.55).

Ссылки

CVE-2023-27522
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CWE-444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27522

MISC
https://httpd.apache.org/security/vulnerabilities_24.html

MISC
https://lists.debian.org/debian-lts-announce/2023/04/msg00028.html

MISC
https://security.gentoo.org/glsa/202309-01

Уязвимость Риск: Недоступно

CVE-2022-36760

Описание

Уязвимость "контрабанды HTTP-запросов" в mod_proxy_ajp HTTP-сервера Apache позволяет переправлять запросы на сервер AJP. Эта проблема затрагивает HTTP-сервер Apache Apache HTTP Server 2.4 версии 2.4.54 и ниже.

Ссылки

CVE-2022-36760
CVSSv3: Базовая оценка 9.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)
CWE-444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36760

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MISC

https://security.gentoo.org/glsa/202309-01

Уязвимость Риск: Недоступно

CVE-2022-37436

Описание

Apache HTTP Server до 2.4.55, вредоносная серверная часть могла привести к преждевременному усечению заголовков ответа, поэтому некоторые заголовки включались в тело ответа. Если более поздние заголовки имеют какую-либо цель обеспечения безопасности, они не будут интерпретированы клиентом.

Ссылки

CVE-2022-37436

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CWE-113
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37436

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MISC

https://security.gentoo.org/glsa/202309-01

Уязвимость Риск: Недоступно

CVE-2023-45802

Описание

Когда поток HTTP/2 был сброшен клиентом (RST кадр), возникло временное окно, в течение которого ресурсы памяти запроса не были восстановлены немедленно. Выделение было отложено до закрытия соединения. Можно отправлять новые запросы и выполнять сброс, сохраняя соединение занятым и открытым и увеличивая объем памяти. Рекомендуется обновиться до 2.4.58.

Ссылки

CVE-2023-45802

CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-400
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-45802
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2MBEPPC36UBVOZZNAXFHKLFGSLCMN5LI/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WE2I52RHNNU42PX6NZ2RBUHSFFJ2LVZX/

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MISC

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BFQD3KUEMFBHPAPBGLWQC34L4OWL5HAZ/

MISC

https://security.netapp.com/advisory/ntap-20231027-0011/

Уязвимость Риск: Недоступно

CVE-2023-31122

Описание

Уязвимость для чтения за пределами доступа в mod_macro HTTP-сервера Apache.Эта проблема затрагивает HTTP-сервер Apache: до 2.4.57.

Ссылки

CVE-2023-31122

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-31122
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ZFDNHDH4VLFGDPY6MEZV2RO5N5FLFONW/

MISC

https://httpd.apache.org/security/vulnerabilities_24.html

MISC

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TI3V2YCEUM65QDYPGGNUZ7UONIM5OEXC/

MISC

https://security.netapp.com/advisory/ntap-20231027-0011/

MISC

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VZJTT5TEFNSBWVMKCLS6EZ7PI6EJYBCO/

Уязвимость Риск: Недоступно

CVE-2022-37454

Описание

Переполнение буфера в Keccak XKCP SHA-3 реализации до 8.0.25 и до 8.1.12 позволяет удалённым злоумышленникам выполнить произвольный код.

Ссылки

CVE-2022-37454

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37454

DEBIAN

https://www.debian.org/security/2022/dsa-5267

DEBIAN

https://www.debian.org/security/2022/dsa-5269

MISC

https://news.ycombinator.com/item?id=33281106

MISC

https://csrc.nist.gov/projects/hash-functions/sha-3-project

MISC

https://mouha.be/sha-3-buffer-overflow/

MISC

https://github.com/XKCP/XKCP/security/advisories/GHSA-6w4m-2xhg-2658

MISC

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/CMIEXLMTW5GO36HTFFWIPB3OHZXCT3G4/

MISC

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3ALQ6BDDPX5HU5YBQOBMDVAA2TSGDKIJ/

MISC

https://eprint.iacr.org/2023/331

MISC

https://news.ycombinator.com/item?id=35050307

MISC

https://security.gentoo.org/glsa/202305-02

MLIST

https://lists.debian.org/debian-lts-announce/2022/10/msg00041.html

MLIST

https://lists.debian.org/debian-lts-announce/2022/11/msg00000.html

Уязвимость Риск: Недоступно

CVE-2022-31628

Описание

Бесконечный цикл в PHP до 7.4.31, 8.0.24 и 8.1.11 при распаковке gzip "quines" файлов.

Ссылки

CVE-2022-31628

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CWE-835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31628

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/XNIEABBH5XCXLFWWZYIDE457SPEDZTXV/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/VI3E6A3ZTH2RP7OMLJHSVFIEQBIFM6RF/

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2L5SUVYGAKSWODUQPZFBUB3AL6E6CSEV/

CONFIRM

https://security.netapp.com/advisory/ntap-20221209-0001/

DEBIAN

https://www.debian.org/security/2022/dsa-5277

GENTOO

https://security.gentoo.org/glsa/202211-03

MISC

https://bugs.php.net/bug.php?id=81726

MLIST

https://lists.debian.org/debian-lts-announce/2022/12/msg00030.html

Уязвимость Риск: Недоступно

CVE-2022-31630

Описание

Уязвимость проверки входных данных в imageloadfont() до 8.0.25 и до 8.1.12.

Ссылки

CVE-2022-31630

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H)
CWE-125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31630

MISC

https://bugs.php.net/bug.php?id=81739

Уязвимость Риск: Недоступно

CVE-2022-31629

Описание

Уязвимость в PHP до 8.0.24 и до 8.1.11 и до 7.4.32 позволяет сайтам злоумышленников установить небезопасный cookie в браузере жертвы.

Ссылки

CVE-2022-31629

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)
NVD-CWE-noinfo
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31629
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/XNIEABBH5XCXLFWWZYIDE457SPEDZTXV/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/VI3E6A3ZTH2RP7OMLJHSVFIEQBIFM6RF/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2L5SUVYGAKSWODUQPZFBUB3AL6E6CSEV/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZGWIK3HMBACERGB4TSBB2JUOMPYY2VKY/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/LSJVPJTX7T3J5V7XHR4MFNHZGP44R5XE/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/KJZK3X6B7FBE32FETDSMRLJXTFTHKWSY/

CONFIRM

https://security.netapp.com/advisory/ntap-20221209-0001/

DEBIAN

https://www.debian.org/security/2022/dsa-5277

GENTOO

https://security.gentoo.org/glsa/202211-03

MISC

https://bugs.php.net/bug.php?id=81727

MLIST

https://lists.debian.org/debian-lts-announce/2022/12/msg00030.html

Уязвимость Риск: Недоступно

CVE-2023-3817

Описание

Отказ в обслуживании в pip пакете cryptography до 41.0.3.

Ссылки

CVE-2023-3817

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CWE-834
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3817
https://security.gentoo.org/glsa/202402-08

MISC

https://www.openssl.org/news/secadv/20230731.txt

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=6a1eb62c29db6cb5eec707f9338aee00f44e26f5

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=9002fd07327a91f35ba6c1307e71fa6fd4409b7f

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=91ddeba0f2269b017dc06c46c993a788974b1aa5

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=869ad69aadd985c7b8ca6f4e5dd0eb274c9f3644

MISC

http://www.openwall.com/lists/oss-security/2023/07/31/1

MISC

http://seclists.org/fulldisclosure/2023/Jul/43

MISC

https://lists.debian.org/debian-lts-announce/2023/08/msg00019.html

MISC

https://security.netapp.com/advisory/ntap-20230818-0014/

MISC

http://www.openwall.com/lists/oss-security/2023/09/22/9

MISC

http://www.openwall.com/lists/oss-security/2023/09/22/11

MISC

https://security.netapp.com/advisory/ntap-20231027-0008/

MISC

http://www.openwall.com/lists/oss-security/2023/11/06/2

Уязвимость Риск: Недоступно

CVE-2023-0466

Описание

Функция X509_VERIFY_PARAM_add0_policy() документирована для неявного включения проверки политики сертификата при проверке сертификата. Однако реализация функции не включает проверку, что позволяет сертификатам с недействительной или неправильной политикой пройти проверку сертификата. Поскольку внезапное включение проверки политики может нарушить существующие развертывания, было решено сохранить существующее поведение функции X509_VERIFY_PARAM_add0_policy(). Вместо этого приложениям, требующим от OpenSSL выполнения проверки политики сертификатов, необходимо использовать X509_VERIFY_PARAM_set1_policies() или явно включить проверку политики, вызвав X509_VERIFY_PARAM_set_flags() с аргументом флага X509_V_FLAG_POLICY_CHECK. Проверка политики сертификатов отключена по умолчанию в OpenSSL и не часто используется приложениями.

Ссылки

CVE-2023-0466

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CWE-295
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0466
https://security.gentoo.org/glsa/202402-08

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=73398dea26de9899fb4baa94098ad0a61f435c72

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=51e8a84ce742db0f6c70510d0159dad8f7825908

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fc814a30fc4f0bc54fcea7d9a7462f5457aab061

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=0d16b7e99aafc0b4a6d729eec65a411a7e025f0a

MISC

https://www.openssl.org/news/secadv/20230328.txt

MISC

https://security.netapp.com/advisory/ntap-20230414-0001/

MISC

https://www.debian.org/security/2023/dsa-5417

MISC

https://lists.debian.org/debian-lts-announce/2023/06/msg00011.html

MISC

http://www.openwall.com/lists/oss-security/2023/09/28/4

Уязвимость Риск: Недоступно

CVE-2022-4450

Описание

Уязвимость двойного освобождения в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t может привести к падению приложения.

Ссылки

CVE-2022-4450

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4450
https://security.gentoo.org/glsa/202402-08

MISC

https://www.openssl.org/news/secadv/20230207.txt

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=63bcf189be73a9cc1264059bed6f57974be74a83

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=bbcf509bd046b34cca19c766bbddc31683d0858b

Уязвимость Риск: Недоступно

CVE-2024-0727

Описание

Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack

Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.

A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue.

OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass().

We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant.

The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

Ссылки

CVE-2024-0727

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)
NVD-CWE-noinfo
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0727
https://www.openssl.org/news/secadv/20240125.txt
https://github.com/openssl/openssl/commit/775acfdbd0c6af9ac855f34969cdab0c0c90844a
https://github.com/openssl/openssl/commit/d135eeab8a5dbf72b3da5240bab9ddb7678dbd2c
https://github.com/openssl/openssl/commit/09df4395b5071217b76dc7d3d2e630eb8c5a79c2
https://github.openssl.org/openssl/extended-releases/commit/03b3941d60c4bce58fab69a0c22377ab439bc0e8
https://github.openssl.org/openssl/extended-releases/commit/aebaa5883e31122b404e450732dc833dc9dee539
https://security.netapp.com/advisory/ntap-20240208-0006/

Уязвимость Риск: Недоступно

CVE-2022-4304

Описание

Уязвимость в IBM Semeru до 8.0.362 и до 11.0.18 и до 17.0.6.

Ссылки

CVE-2022-4304

CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
CWE-203
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4304
https://security.gentoo.org/glsa/202402-08

MISC

https://www.openssl.org/news/secadv/20230207.txt

Уязвимость Риск: Недоступно

CVE-2023-0286

Описание

Уязвимость, связанная с подменой типа в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t при обработке X.509 GeneralName может позволить злоумышленнику передать произвольные указатели на вызов memcmp и прочитать содержимое памяти или вызвать отказ в обслуживании.

Ссылки

CVE-2023-0286

CVSSv3: Базовая оценка 7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H)
CWE-843
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0286
https://security.gentoo.org/glsa/202402-08

MISC

https://www.openssl.org/news/secadv/20230207.txt

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2c6c9d439b484e1ba9830d8454a34fa4f80fdfe9

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2f7530077e0ef79d98718138716bc51ca0cad658

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fd2af07dc083a350c959147097003a14a5e8ac4d

MISC

https://ftp.openbsd.org/pub/OpenBSD/LibreSSL/libressl-3.6.2-relnotes.txt

MISC

https://ftp.openbsd.org/pub/OpenBSD/patches/7.2/common/018_x509.patch.sig

Уязвимость Риск: Недоступно

CVE-2023-0465

Описание

Приложения, использующие при проверке сертификатов опции не по умолчанию, могут быть уязвимы для атаки со стороны вредоносного ЦС с целью обхода определенных проверок. Недействительные политики сертификата в листовых сертификатах молча игнорируются OpenSSL, и другие проверки политики сертификата для этого сертификата пропускаются. Вредоносный ЦС может использовать это для намеренного утверждения недействительных политик сертификата, чтобы полностью обойти проверку политики сертификата. Обработка политик отключена по умолчанию, но может быть включена путем передачи аргумента `-policy' утилитам командной строки или вызовом функции `X509_VERIFY_PARAM_set1_policies()'.

Ссылки

CVE-2023-0465

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CWE-295
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0465
https://security.gentoo.org/glsa/202402-08

MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=facfb1ab745646e97a1920977ae4a9965ea61d5c
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=1dd43e0709fece299b15208f36cc7c76209ba0bb
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=b013765abfa80036dc779dd0e50602c57bb3bf95
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=10325176f3d3e98c6e2b3bf5ab1e3b334de6947a
MISC
https://www.openssl.org/news/secadv/20230328.txt
MISC
https://security.netapp.com/advisory/ntap-20230414-0001/
MISC
https://www.debian.org/security/2023/dsa-5417
MISC
https://lists.debian.org/debian-lts-announce/2023/06/msg00011.html

Уязвимость Риск: Недоступно

CVE-2023-5678

Описание

Генерация чрезмерно длинных ключей X9.42 DH или проверка чрезмерно длинных ключей или параметров X9.42 DH может выполняться очень медленно.

Ссылки

CVE-2023-5678
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CWE-754
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5678
https://security.netapp.com/advisory/ntap-20231130-0010/
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=710fee740904b6290fef0dd5536fbcedbc38ff0c
MISC
https://www.openssl.org/news/secadv/20231106.txt
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=db925ae2e65d0d925adef429afc37f75bd1c2017
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=ddeb4b6c6d527e54ce9a99cba785c0f7776e54b6
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=34efaef6c103d636ab507a0cc34dca4d3aecc055

Уязвимость Риск: Недоступно

CVE-2023-0464

Описание

Уязвимость в OpenSSL 3.1.0 до 3.1.1, 3.0.0 до 3.0.9, и 1.1.1 до 1.1.1u, связанная с проверкой X.509 сертификата, позволяет вызвать отказ в обслуживании (DoS) через злонамеренный сертификат.

Ссылки

CVE-2023-0464
CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-295
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0464
https://www.couchbase.com/alerts/
https://security.gentoo.org/glsa/202402-08

MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1
MISC
https://www.openssl.org/news/secadv/20230322.txt
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2dcd4f1e3115f38cefa43e3efbe9b801c27e642e
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=879f7080d7e141f415c79eaa3a8ac4a3dad0348b
MISC
https://www.debian.org/security/2023/dsa-5417
MISC
https://lists.debian.org/debian-lts-announce/2023/06/msg00011.html

Уязвимость Риск: Недоступно

CVE-2023-3446

Описание

Отказ в обслуживании в pip пакете cryptography до 41.0.3.

Ссылки

CVE-2023-3446
CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CWE-1333
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3446
https://security.gentoo.org/glsa/202402-08
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fc9867c1e03c22ebf56943be205202e576aabf23
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8780a896543a654e757db1b9396383f9d8095528
MISC
https://www.openssl.org/news/secadv/20230719.txt
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=9a0a4d3c1e7138915563c0df4fe6a3f9377b839c
MISC
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=1fa20cf2f506113c761777127a38bce5068740eb
MISC
http://www.openwall.com/lists/oss-security/2023/07/19/5
MISC
http://www.openwall.com/lists/oss-security/2023/07/19/4
MISC
http://www.openwall.com/lists/oss-security/2023/07/19/6
MISC
http://www.openwall.com/lists/oss-security/2023/07/31/1
MISC
https://security.netapp.com/advisory/ntap-20230803-0011/
MISC
https://lists.debian.org/debian-lts-announce/2023/08/msg00019.html

Уязвимость Риск: Недоступно

CVE-2023-4807

Описание

Отказ в обслуживании в pip пакете cryptography до 41.0.4.

Ссылки

CVE-2023-4807

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
NVD-CWE-noinfo
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4807

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=a632d534c73eeb3e3db8c7540d811194ef7c79ff

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=4bfac4471f53c4f74c8d81020beb938f92d84ca5

MISC

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=6754de4a121ec7f261b16723180df6592cbb4508

MISC

https://www.openssl.org/news/secadv/20230908.txt

MISC

https://security.netapp.com/advisory/ntap-20230921-0001/

Конец отчёта. RedCheck 2.6.9.6467.
RedCheckID: 70AD472E-4D3F-4A9E-B505-BA2B8BD2B5A5.